FATTMERCHANT, INC.
DBA STAX

SOC 2 REPORT

FOR

STAX, CARDX AND STAX BILL

A TYPE 2 INDEPENDENT SERVICE AUDITOR'S REPORT ON CONTROLS RELEVANT TO SECURITY, AVAILABILITY, PROCESSING INTEGRITY, AND CONFIDENTIALITY

SEPTEMBER 1, 2022, TO MARCH 31, 2023

Attestation and Compliance Services

This report is intended solely for use by the management of Fattmerchant, Inc. DBA Stax, user entities of Fattmerchant, Inc.'s DBA Stax services, and other parties who have sufficient knowledge and understanding of Fattmerchant, Inc.'s DBA Stax services covered by this report (each referred to herein as a "specified user").

If report recipient is not a specified user (herein referred to as a "non-specified user"), use of this report is the non-specified user's sole responsibility and at the non-specified user's sole and exclusive risk. Non-specified users may not rely on this report and do not acquire any rights against Schellman & Company, LLC as a result of such access. Further, Schellman & Company, LLC does not assume any duties or obligations to any non-specified user who obtains this report and/or has access to it.

Table of Contents

SECTION I

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Fattmerchant, Inc. DBA Stax:

Scope

We have examined Fattmerchant, Inc.'s DBA Stax ("Stax" or the "service organization") accompanying description of its Stax, CardX and Stax Bill applications system, in Section 3, throughout the period September 1, 2022, to March 31, 2023, (the "description"), based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) ("description criteria") and the suitability of the design and operating effectiveness of controls stated in the description throughout the period September 1, 2022, to March 31, 2023, to provide reasonable assurance that Stax Payment's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity and confidentiality ("applicable trust services criteria") set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

Stax uses various subservice organizations for cloud and data center hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Stax, to achieve Stax' service commitments and system requirements based on the applicable trust services criteria. The description presents Stax' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Stax' controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The information included in Section 5, "Other Information Provided by Stax" is presented by Stax' management to provide additional information and is not a part of the description. Information about Stax management's responses to exceptions noted has not been subjected to the procedures applied in the examination of the description, the suitability of the design of controls, and the operating effectiveness of the controls to achieve Stax' service commitments and system requirements based on the applicable trust services criteria.

Service Organization's Responsibilities

Stax is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Stax' service commitments and system requirements were achieved. Stax has provided the accompanying assertion, in Section 2, ("assertion") about the description and the suitability of design and operating effectiveness of controls stated therein. Stax is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements;
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively;
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria;
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria;
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria; and
- Evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Test of Controls

The specific controls we tested, and the nature, timing, and results of those tests are presented in Section 4 of our report titled "Testing Matrices."

Opinion

In our opinion, in all material respects,

a. the description presents Stax' Stax, CardX and Stax Bill application system that was designed and implemented throughout the period September 1, 2022, to March 31, 2023, in accordance with the description criteria;

b. the controls stated in the description were suitably designed throughout the period September 1, 2022, to March 31, 2023, to provide reasonable assurance that Stax' service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization applied the complementary controls assumed in the design of Stax' controls throughout that period; and

c. the controls stated in the description operated effectively throughout the period September 1, 2022, to March 31, 2023, to provide reasonable assurance that Stax' service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls assumed in the design of Stax' controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of Stax; user entities of Stax' Stax, CardX and Stax Bill applications system during some or all of the period September 1, 2022, to March 31, 2023, business partners of Stax subject to risks arising from interactions with the Stax, CardX and Stax Bill application system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization;
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties;
- Internal control and its limitations;
- Complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements;
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services;
- The applicable trust services criteria; and
- The risks that may threaten the achievement of the service organization's service commitments and system requirements, and how controls address those risks.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

Schellman & Company, LLC

Tampa, Florida
June 8, 2023

SECTION 2

MANAGEMENT'S ASSERTION

MANAGEMENT'S ASSERTION

We have prepared the accompanying description of Fattmerchant, Inc.'s ("Stax") Stax, CardX and Stax Bill application system, in Section 3, during the period September 1, 2022, to March 31, 2023, (the "description") based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), ("description criteria"). The description is intended to provide report users with information about the Stax, CardX and Stax Bill application system that may be useful when assessing the risks arising from interactions with Stax' system, particularly information about system controls that Stax has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, and confidentiality ("applicable trust services criteria") set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

Stax uses various subservice organizations for cloud and data center hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Stax, to achieve Stax' service commitments and system requirements based on the applicable trust services criteria. The description presents Stax' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Stax' controls. The description does not disclose the actual controls at the subservice organizations.

We confirm, to the best of our knowledge and belief, that:

a. the description presents Stax' Stax, CardX and Stax Bill application system that was designed and implemented during the period September 1, 2022, to March 31, 2023, in accordance with the description criteria;

b. the controls stated in the description were suitably designed throughout the period September 1, 2022, to March 31, 2023, to provide reasonable assurance that Stax' service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations applied the complementary controls assumed in the design of Stax' controls throughout that period; and

c. the controls stated in the description operated effectively throughout the period September 1, 2022, to March 31, 2023, to provide reasonable assurance that Stax' service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls assumed in the design of Stax' controls operated effectively throughout that period.

SECTION 3

DESCRIPTION OF THE SYSTEM

Overview of Operations

Company Background

Headquartered in Orlando, Florida, Fattmerchant, Inc. DBA Stax was founded in 2014. Stax offers a suite of payment processing solutions, including credit card processing, mobile payments, and e-commerce solutions.

The company has over 30,000+ merchants enrolled in the platform and since its inception, Stax has powered more than $30 billion in transactions. Payment transactions are supported by payment facilitators and processors in the country allowing for greater flexibility and resiliency to serve our merchant's needs.

Since its founding, Stax has been located in Orlando, Florida. Multiple expansions over the last two years support the rapid growth the company still enjoys today. Remote strategic staff help support the company vision of providing world class service to their customers and partners.

Description of Services Provided

Stax

Stax is a payment processing company that offers a range of solutions for businesses to accept credit card payments. Stax is the primary product offering of the company, which provides a full-service payment processing solution for businesses. Stax enables businesses to accept credit card payments in various ways, including in-store, online, and on-the-go. The company offers a range of features, including customizable reporting, fraud protection, integrations with popular accounting software, and a subscription-based pricing model for businesses of all sizes. Overall, Stax is designed to make it easy and affordable for businesses to accept credit card payments, while providing them with the tools and features they need to manage their payments efficiently and securely.

CardX

CardX is a payment processing application that offers a solution to help businesses accept credit card payments while passing the cost of processing fees directly to the cardholder. This means that businesses can accept credit card payments without paying any processing fees themselves, potentially saving them a significant amount of money. The way CardX accomplishes this is through their patented technology, which adds a transparent fee to the cardholder's transaction. This fee is fully disclosed to the cardholder before they complete the transaction, so they can choose to accept the fee or pay with a different payment method if they prefer. CardX also provides a range of features and integrations, including online payment solutions, invoicing, and recurring billing, to help businesses manage their payment processes more efficiently.

Stax Bill

Stax Bill is a billing and invoicing software solution for businesses. Stax Bill enables businesses to create and send customized invoices, track payments, and manage their billing and invoicing processes. Stax Bill, businesses can automate many of their billing tasks, such as recurring invoices and payment reminders. Stax Bill also includes features such as real-time reporting and analytics, enabling businesses to track their invoicing and payment activities and gain insights into their financial performance. Stax Bill is designed to help businesses manage their billing and invoicing processes and improve their cash flow.

Principal Service Commitments and System Requirements

Commitments are declarations made by management to customers regarding the performance of the Stax, CardX, and Stax Bill application system. Commitments are documented and communicated in standardized contracts and service level agreements.

System requirements are specifications regarding how the Stax, CardX, and Stax Bill application system should function to meet Stax' principal commitments to user entities. System requirements are specified in Stax' policies and procedures, which are available to all employees.

Stax' principal service commitments and system requirements related to the Stax, CardX, and Stax Bill applications system include the following.

Principal Service Commitments and System Requirements		
Trust Services Category	**Service Commitments**	**System Requirements**
Security	• System access is granted to authorized personnel only • Protection of data at rest and in transit • Regular security assessments • Identification and remediation of security incidents/events • Regular system updates • Protection of personally identifying information and security of the information system from unauthorized access, use, modification, disclosure, destruction, threats, or hazards • Develop, implement, and maintain an information security program designed to protect the security, integrity, and confidentiality of the system and its information • Perform risk assessments for both internal and external threats to the system and its information • Enable timely, reliable, and continuous access to and use of information and systems to support operations • Develop and maintain secure applications	• Logical access standards • Physical access standards • Employee provisioning and deprovisioning standards • Access reviews • Encryption standards • Intrusion detection and prevention standards • Risk and vulnerability management standards • Configuration management • Incident handling standards • Change management standards • Vendor management
Availability	• Redundancies to allow failover in the event of certain system failures or outages. Ability to recover and restore customer data • 4 hour Recovery Time Objective (RTO) / Recovery Point Objective (RPO) • Communicate system performance and uptime and provide transparency	• System monitoring • Backup and recovery standards • Physical and environmental protections

Principal Service Commitments and System Requirements		
Trust Services Category	**Service Commitments**	**System Requirements**
Processing Integrity	• Create a risk management program to oversee and monitor transactions • Implement processing integrity incident management procedures and lessons learned for timely resolution and continuous improvement • Provide merchants and partners with reporting, dashboards, and data to provide visibility and transparency into transaction processing	• Transaction processing monitoring and management • Help desk ticketing system
Confidentiality	• Maintain all customer data as confidential and not to disclose information to any unauthorized parties without written consent	• Data classification • Retention and destruction standards • Data handling standards • Internal confidentiality standards • Information sharing standards

In accordance with Stax' assertion, and the description criteria, the aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to all system users, in each individual case.

COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICE

System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

Infrastructure and Software

Stax and CardX have been built exclusively using current cloud-native solutions. The applications leverage Infrastructure as a Service (IaaS) capabilities to support resiliency, scalability, security, and operational integrity. The design uses containers and hosts to quickly scale services to support unexpected load peaks. The physical infrastructure and security are maintained by AWS and the configuration of networking, services, backups, applications, and encryption are configured by Stax.

Stax Bill uses data center configuration in the Rogers data center in Ottawa, Canada. The environment is configured using high availability and redundancy and is monitored to verify the resources are appropriate for the usage and customer base.

Stax, CardX and Stax Bill are centrally monitored by the enterprise information security team, risk team, and core technology team. The cloud environment is monitored using cloud configuration monitoring tools to detect

misconfigurations and deviations from recommendations from AWS and security groups. The cloud environments leverage cloud native solutions such as AWS-managed databases, including backups. The data in the cloud environment is encrypted using customer-managed keys to provide a higher level of confidentiality. Container technology is also used in the cloud environment, along with cross availability zone (multiple data centers) to support the application in the event of a local outage. The applications for Stax Bill are built using the .net framework and the Microsoft ecosystem such as MS SQL Server and Active Directory. Database environments for Stax Bill are configured to failover to a secondary database in the case of an outage.

Firewall rules and security groups are configured for all environments to restrict traffic unless explicitly allowed. Firewall rules are configured on firewalls for the Stax Bill environment and security groups are configured for the AWS environment. Additionally, a web application firewall is in place to monitor application traffic, detect and block potential threats. Intrusion detection systems are in place to monitor network traffic and alert IT personnel of potential security events.

The in-scope infrastructure consists of multiple applications, operating system platforms and databases, as shown in the table below:

Primary Infrastructure			
Production Application	**Business Function Description**	**Operating System Platform**	**Physical Location**
paymentplatformapi.fusebill.com	Primary payment web application	Windows Server 2012 R2	Rogers DC
Stax Bill Custom Vault	Vault and encryption service		
Stax Bill Custom Key	Vault key holder service		
Stax Bill Custom Vault Manager	Vault and keyholder management application		
Stax Bill Custom Web Application (admin.staxbill.com)	Customer web user interface		
Stax Bill Custom Web Application (secure.fusebill.com)	Customer API interface		
Stax Bill Custom Web Application (payments.subscriptionplatform.com)	Customer transparent redirect		
Stax Bill Custom Web Application (*.mybillsystem.com)	Customer hosted pages user interface		
Firewall IPS Gateway Anti-Virus SSLVPN Network Segmentation	SonicWALL	NSA 4600 6.5.4.4-44n	
Layer-7 Application Load Balancer	Brocade	Virtual Traffic Manager 11.1	
Hypervisor	HyperV	Windows Server 2012 R2	

Primary Infrastructure			
Production Application	**Business Function Description**	**Operating System Platform**	**Physical Location**
CardX Marketing Site (cardx.com)	Marketing site for attracting new customers	AWS LightSail LAMP (Linux)	AWS us-east-2 (Ohio)
CardX Portal (portal.cardx.com)	App for logged-in clients to manage and see sale and deposit activity	AWS static assets from S3	
CardX Portal API (api.portal.cardx.com)	API used by CardX Portal and interfaced to directly by clients	AWS Lambda (node js runtime)	
CardX Lightbox	Customer facing payment form	AWS static assets from S3	
CardX Lightbox API	API for use by CardX Lightbox	AWS Lambda (node js runtime)	
CardX Card Field	Single UI component to collect card numbers and return card tokens	AWS static assets from S3	
CardX Pricing Technology	Determines surcharge for a given transaction	AWS Lambda (node js runtime)	
CardX Integrations API	API containing custom endpoints for Enterprise clients		
RDS	Database Management System	AWS Aurora RDS	AWS us-west-2
Redshift	Data warehouse	AWS Redshift	
Stax Marketing Site	Marketing database and login front end	AWS S3 single page application	
Stax API	API backend for Stax	AWS ECS	
AWS	Infrastructure as a service (CardX and Stax)	AWS multiple services	

People

Personnel involved in the operation and use of the system are:

- Executive Management – responsible for overseeing company-wide activities, establishing, and accomplishing goals, and overseeing objectives.
- Human Resources (HR) – responsible for HR policies, practices, and processes with a focus on key HR department delivery areas (e.g., talent acquisitions, employee retention, compensation, employee benefits, performance management, employee relations and training, and development).

- IT Personnel – responsible for the onboarding and offboarding of staff, contractors and internal users of applications, technology, and network connected assets.
- Security and Compliance - responsible for setting the requirements for the company in the designing, implementing, and monitoring of applications developed or used by Stax.
- Operations - supports Stax by ensuring the onboarding, activation, service, expansion, and retention for our new and existing members.
- Quality Assurance - responsible for creating and implementing quality assurance strategies for all internally developed products.
- Cloud Engineering - responsible for all the AWS and Cloud resource deployments - including other vendors like Cloudflare.

Procedures

Access, Authentication, and Authorization

Documented logical access policies and standard build procedures are in place to guide personnel in information security practices that include, but are not limited to, password requirements, access provisioning, access termination, and the installation and maintenance of production servers. Access to system information by personnel is protected by two factor authentication and authorization mechanisms via Okta. Account management is managed within Google for Stax and CardX. Domain accounts and privileges are used to manage the Stax Bill environment. The production environment of the applications is administered remotely with authentication requiring users to first authenticate to the production VPN system via a username, password and two factor authentication. VPN sessions are encrypted. Once connected to the production VPN, users can access the production environments based on their role and authorized access.

The production environment for Stax and CardX is hosted within AWS while the production environment for Stax Bill is hosted on site in the Rogers datacenter. For all systems, predefined security groups are utilized to assign role-based access privileges and segregate access to data to the in-scope application. Administrative access privileges are assigned to only those users requiring access to fulfill their job responsibilities and are restricted to authorized personnel.

Access Requests and Access Revocation

Access management policies and procedures are in place to guide personnel in the access provisioning and deprovisioning process. Access requests for new hires are submitted by HR and fulfilled by IT. Access is provisioned based on predefined access matrix which includes required systems and privileges for specific user roles. If additional access is required, employee's managers must submit additional access requests for additional access. Access revocation tickets are submitted to IT personnel and are utilized to track access revocation of the terminated employee. Access reviews are performed on a quarterly basis to ensure that no terminated users accounts are still active within any of the systems. Accounts identified as inappropriate are investigated and resolved.

Physical Access

Physical access policies and procedures are in place to guide personnel in the use of authorized access to the physical data center environment. Physical access to the data center is restricted to authorized personnel. Rogers data center is responsible for managing physical controls at the datacenter.

Change Management

The change management process is used to ensure that changes to the product and system are introduced in a controlled and coordinated manner. Documented application change management policies and procedures are in place to guide personnel in the request, documentation, testing, and approval of system changes. Change management documents including policies, procedures, and guidance documents are documented on an internal document repository. Change management architecture review meetings are held on a weekly basis to discuss and communicate the ongoing and upcoming projects that affect the system. Production changes are documented and tracked in a ticketing system. Changes are categorized and follow specific approval paths based on the type

and importance of the change. Version control software is utilized to control changes to developed applications and provide rollback capabilities. Access to modify source code contained in the version control software is restricted to those with a business need. Separate development, testing, and production environments are maintained.

By policy, certain changes are tested in the test environment prior to implementation. The production change request process enforces and records request authorization, review, approval, and testing (where applicable). Approval for releases is obtained prior to moving the changes to production. Specific roles in the organization have been assigned the roles for approving and signing off before changes can be promoted to production.

Data Backup and Disaster Recovery

Documented policies and procedures are in place to guide personnel in performing system backup and restoration activities. An automated backup system is configured to perform daily backups of production data. The automated backup system is configured to log the backup job completion status for backups and send alert notifications to IT operations personnel regarding the success or failure of the backup jobs. The automated backup system is configured to encrypt backup data and log backup job completion status. E-mail alert notifications are sent to IT personnel in the event of a failed backup job. Data restoration activities from backup images are performed on an ad hoc basis as a component of business operations. Enterprise monitoring applications are utilized to monitor the performance and availability of the production environment and associated system resources. The monitoring applications are configured to send notifications to IT personnel when predefined thresholds are exceeded on monitored systems.

Stax has developed a disaster recovery plan (DRP). The purpose of the DRP is to prepare employees in the event of extended service outages caused by factors beyond Stax control (e.g., natural disasters, man-made events), and to restore services to the widest extent possible in a minimum time frame. Stax has implemented preventive measures whenever possible to minimize operational disruptions and to recover as rapidly as possible when an incident occurs. Disaster recovery plan and tabletop testing activities are performed at least annually.

Incident Response

Documented incident management and response procedures are in place to guide personnel in identifying, reporting, and handling unexpected incidents impacting the business. The procedures are reviewed on a periodic basis to ensure they are still effective in meeting the business objectives. The procedures outline the following:

- Assignment of roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program
- Containment of the incident and threat
- Eradication and remediation of the incident
- Recovery for restoration of operations
- Follow-up phase including lessons learned

The policies and procedures define incidents as any real or suspected adverse event in relation to the security of computer systems or computer networks, events which causes or may have an impact on confidentiality or integrity of company or customer data or any event that has an adverse impact on the company's reputation as a trusted owner of data. Stax has established a computer incident response team (CIRT) to help prevent and minimize material loss to the organization's information assets and systems as a result of an adverse security or privacy incident. The CIRT's primary role is to aid the detection, reporting, investigation, and resolution of security and privacy incidents occurring on Stax computers, applications, or networks. In addition, the CIRT provides guidance and education to employees, which is designed to reduce incidents. In the event of a verified adverse event, or an incident, the CIRT has the authority to invoke the incident response plan and undertake the necessary actions or decisions to protect and restore Stax computers, applications, or network infrastructure. A ticketing system is utilized for documenting, communicating, and collaborating to resolve any identified incidents with customers. A root cause analysis is performed for incidents that includes an impact analysis, resolution, lessons learned, and action items. Corrective measures or changes that occur as a result of incidents and identified deficiencies follow the standard change control process.

System Monitoring

Enterprise monitoring applications are utilized to monitor the back-end processing performance and availability of the application and associated system resources. The monitoring applications are configured to notify IT operations personnel via on-screen and e-mail notifications when predefined thresholds are exceeded on monitored systems including timeout thresholds for database replication latency.

In the event of an application outage, the system is configured to alert application support personnel regarding potential system errors or outages during system processing. A service status monitoring dashboard is made available via a public facing website to communicate current service availability, system uptime metrics, processing issues and outages is made available to end-users.

Data

By design Stax, Cardx and Stax Bill minimize the collection of sensitive information to what is needed to provide the service to the customers. Stax, CardX, and Stax Bill use Customer Relationship Management (CRM) tools to identify prospective customers, maintain a history of requests, and collect information needed to onboard and underwrite customers (merchants). The information in the CRM often contains personally identifiable information (PII) which is needed to perform underwriting as required by contractual agreements with financial institutions and regulatory bodies. Attachments with the most sensitive information are stored in the internally built application using encrypted object storage and accessible only by specific roles such as underwriting role internal user.

Transactions are tokenized prior to being transmitted through the system to prevent the need to have cardholder data for Stax and CardX. Transaction data includes e-mails, phone numbers, transaction tokens, and pertinent financial information such as transaction billed amount.

Transactions for Stax Bill may include cardholder information which is stored in a transaction vault that is segregated from the rest of the network.

There is separate object storage for Stax and CardX in completely segregated AWS accounts that are purpose-built only to host PCI information. These data objects contain cardholder information sent from acquirers for reporting. An internal process masks and strips the cardholder data before it is added to the database.

Transaction information may be corrected using tickets into support which may trigger DevOps teams to perform updates as needed. Other changes may be performed by operations staff, which are tracked via tickets and internally in system monitoring tools. Examples of this are token migrations from previous payment processors, changes in ownership, etc.

The following table describes the information used and supported by the system.

Data Used and Supported by the System		
Data Description	**Data Reporting**	**Classification**
Merchant database (Stax, CardX, Stax Bill)	Obtained during onboarding, and as part of requests from merchants. Data is maintained by Sales Operations and reported to senior leadership.	Confidential
Transaction database (Stax Bill)	Transaction information including cardholder information.	
Transaction database (Stax, Cardx)	Transaction information not including cardholder information.	
Reporting database (Stax, CardX, Stax Bill)	Information used by merchants and internal support staff to support merchants.	

Data Used and Supported by the System		
Data Description	**Data Reporting**	**Classification**
Transaction Report File (Stax, CardX)	Report of transactions form acquirer includes cardholder data.	Confidential

Significant Changes During the Period

There were no significant changes that are likely to affect report users' understanding of how the in-scope system is used to provide the services covered by this examination during the period.

Subservice Organizations

The cloud hosting and data center hosting services provided by AWS and Rogers were not included within the scope of this examination.

The following table presents the applicable Trust Services criteria that are intended to be met by controls at AWS and Rogers, alone or in combination with controls at Stax, and the types of controls expected to be implemented at AWS and Rogers to achieve Stax principal service commitments and system requirements based on the applicable trust services criteria.

Control Activities Expected to be Implemented by AWS and Rogers	Applicable Trust Services Criteria
AWS is responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Stax application systems reside.	CC6.1, CC6.2, CC6.3, CC6.5, CC6.6, CC7.2
AWS and Rogers are responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers.	CC6.4, CC6.5, CC7.1
AWS is responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices for its cloud hosting services where Stax systems reside.	CC6.7
AWS is responsible for monitoring any changes to the logical access controls system for the underlying network, virtualization management, and storage devices where the Stax application systems reside.	CC7.1
AWS and Rogers are responsible for designing, developing, implementing, operating, maintaining, and monitoring the environmental control systems at the data center facility where the Stax application systems reside. AWS and Rogers are also responsible implementing recovery controls for failover to infrastructure located at an alternative facility in the event of a disaster or emergency event.	A1.2

Control Environment

The control environment at Stax is the foundation for the other areas of internal control. It sets the tone of the organization and influences the control consciousness of its personnel. The components of the control environment factors include the integrity and ethical values, management's commitment to competence; its organizational structure; the assignment of authority and responsibility; and the oversight and direction provided by the board of directors and operations management.

Integrity and Ethical Values

Integrity and ethical values are essential elements of the control environment, affecting the design, administration, and monitoring of key processes. Integrity and ethical behavior are the products of Stax' ethical and behavioral standards, how they are communicated, monitored, and enforced in its business activities. They include communication of the company's values and behavioral standards to personnel through policy statements and codes of conduct, and by the examples the executives set.

The senior executive team and management recognize their responsibility to foster a strong ethical environment within Stax to determine that its business affairs are conducted with integrity, and in accordance with high standards of personal and corporate conduct. This responsibility is characterized and reflected in the Stax' Code of Conduct, which is distributed to all employees of the organization. Specifically, employees and their immediate families are prohibited from using their positions with Stax for personal or private gain, disclosing confidential information regarding clients, or taking any action that is not in the best interest of clients. All employees are required to maintain ongoing compliance with all statements of policies, procedures, and standards of the Code of Conduct and with lawful and ethical business practices, whether or not they are specifically mentioned in the Code of Conduct. Each employee is required to affirm annually that he or she received, read, understood, and complied with the requirements set forth in the Code of Conduct and the Employee Handbook. Employee recertification status is monitored periodically for compliance.

Direction for the organization is set at the executive management level. Security, compliance, and adherence to company values are influenced by a conscious and supportive senior management who seek to provide the right balance of oversight and autonomy to empower the organization to meet company goals and objectives. Specific control activities that Stax has implemented in this area are described below:

- The employee handbook developed and communicated to the entire workforce contains the policies, procedures, and organizational approach for the organization, including mechanism used to hold individual contributors accountable for alignment with the company.
- Employees are required to acknowledge the employee handbook upon hire indicating they have been given access to the employee handbook and understand their responsibility for adhering to the associated policies and procedures.
- Background checks are performed on employees as a component of the hiring process to ensure candidates have sufficient qualifications and technical competency.

Board of Directors and Executive Management Oversight

An entity's control consciousness is influenced significantly by the entity's board of directors and executive management. The board of directors' charter documents the responsibilities of the board. Stax' board of directors and executive management meet on at least a quarterly basis to monitor Stax' internal control performance, financials, regulatory, auditor report and communicate any issues identified.

Organizational Structure and Assignment of Authority and Responsibility

Stax' organizational structure provides the framework within which its activities for achieving company-wide objectives are planned, executed, controlled, and monitored. Stax' management believes that establishing a relevant organizational structure includes considering key areas of authority, responsibility, and appropriate lines of reporting. Stax has developed an organizational structure suited to its needs. This organizational structure is based, in part, on its business unit's size and the nature of its activities.

Stax assignment of authority and responsibility activities includes factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, Knowledge and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring that personnel understand Stax' objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable. Management utilizes organizational charts to communicate key areas of authority, responsibility, and lines of reporting. Specific control activities that

Stax has implemented in this area are described below:

- The organizational structure, reporting lines, and authorities are defined in organizational charts, updated on an as-needed basis, and communicated to employees.
- Documented job descriptions are in place and include expectations and responsibility of employees for their organizational unit.
- The board of directors' meetings are held on a quarterly basis to review internal control performance, financials, regulatory, auditor report and communicate any issues identified.

Commitment to Competence

Stax' management team defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Stax' commitment to competence includes management's consideration of the competence levels for jobs and how those levels translate required skills and knowledge levels into written position requirements. Specific control activities that Stax has implemented in this area are described below:

- HR documents the organizational approach within policies and procedures for performing workforce evaluations of employees.
- Organizational leaders perform performance evaluations annually to evaluate the employee against company values, role specific goals and other management defined goals.
- Background checks are performed on employees as a component of the hiring process to ensure candidates have sufficient qualifications and technical competency.
- Established talent management policies and procedure are in place which defines the requirements which need to be fulfilled, in order to be hired for a position within the company.
- Documented job descriptions are in place and include expectations and responsibility of employees for their organizational unit.
- The entity maintains a centralized knowledge base with the information and training required by individual contributors to perform their work functions.

Accountability

The management philosophy and operating style at Stax encompasses a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks, and management's attitudes toward information processing, accounting functions, and personnel. HR policies and practices have been developed to define employee hiring, evaluation, training, and disciplinary processes. Management establishes accountability by holding parties responsible for internal control responsibilities. Specific control activities that Stax has implemented in this area are described below:

- The board of directors and executive management meet on at least a quarterly basis to monitor internal control performance, financials, regulatory, auditor report and communicate any issues identified.
- Documented job descriptions are in place and include expectations and responsibility of employees for their organizational unit.
- Organizational leaders perform performance evaluations annually to evaluate the employee against company values, role specific goals and other management defined goals.
- The employee handbook developed and communicated to the entire workforce contains the policies, procedures, and organizational approach for the organization, including mechanism used to hold individual contributors accountable for alignment with the company.
- Employees are required to acknowledge the employee handbook upon hire indicating they have been given access to the employee handbook and understand their responsibility for adhering to the associated policies and procedures.

RISK ASSESSMENT

Objective Setting

Stax' risk assessment process involves an active process for identifying and analyzing risks that threaten the organization's ability to perform the services within scope. The process starts first with determining the organization's objectives as these are key to understanding, assessing, and putting into effect action needed to address the risks relative to the objectives. Management has committed to carry out certain objectives in relation to the services provided. Stax' commitments and IT operational, reporting, compliance objectives for risk mitigation, data protection, regulatory and legal compliance are formally documented in the information security and privacy policies. The VP of IT and security reviews the commitments and objectives related to data security, availability, integrity, and confidentiality on an annual basis. Management also holds a quarterly meeting to discuss and align internal control responsibilities, performance measures and incentives with company objectives.

Risk Identification and Analysis

Stax has considered the significant interactions between itself and relevant external parties and risks that could affect the organization's ability to provide reliable service to its user entities. The VP of IT and security is responsible for overseeing the risk assessment process and coordinating with key members of the executive management, IT, and operational teams to identify and review risks to the system. Meetings with risk stakeholders are held at least annually, and include the evaluation of control activities, business and security risks, vulnerabilities, laws, and regulations. Risk assessment activities include the analysis of potential threats and vulnerabilities arising from vendors providing goods and services, as well as threats and vulnerabilities arising from business partners, customers, and others with access to the entity's information system. Security reviews and vulnerability assessments, are also performed by IT personnel and third-party vendors on a periodic basis to identify threats and assess their potential impact to the system. Risks identified during the assessments are documented within help desk tickets to ensure tracking to resolution.

Stax has documented policies and procedures in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process. Risks are prioritized by risk score, and reviewed by IT management, responsible for how the risk should be managed. This involves judgment based on assumptions about the risk, and reasonable analysis of costs associated with reducing the level of risk. Necessary actions are taken to reduce the significance or likelihood of the risk occurring and identify the control activities necessary to mitigate the risk.

Risk Factors

Management considers risks that can arise from both external and internal factors including the following:

External Factors

- Technological developments
- Changing customer needs or expectations
- Competition that could alter marketing or service activities
- New legislation and regulation that could force changes in policies and strategies
- Natural catastrophes that could lead to changes in operations or information systems
- Economic changes that could have an impact on management decisions

Internal Factors

- Significant changes in policies, processes, or personnel
- Types of fraud

- Fraud incentives and pressures for employees
- Fraud opportunities
- Employee attitudes and rationalizations for fraud
- A disruption in information systems processing
- The quality of personnel hired, and methods of training utilized
- Changes in management responsibilities

Potential for Fraud

The potential for fraud is included within the risk assessment process. The risks are rated using a risk evaluation process and documented within the risk register. Mitigation plans are proposed, and the risk register is reviewed by the senior leadership team and board of directors on at least an annual basis.

Risk Mitigation

Risk mitigation activities include the ability to identify, select and develop activities that sufficiently meet the identified risks, and the organization has documented policies and procedures to guide personnel during this process. Risk identification and mitigation activities performed during the annual risk assessment process also consider the risks that could arise from potential business disruptions caused by an unexpected event.

Vendors and business partners are also considered during the risk assessment and mitigation activities. To assist with this process, vendor management policies are in place to guide personnel in the organization's data protection and handling requirements for third-party provider contracts and due diligence for the performance of periodic compliance monitoring activities. A risk assessment is performed on an annual basis that considers risks associated with vendors and business partners. Risks that are identified are rated using a risk evaluation process and are formally documented, along with mitigation strategies, for management review. Additionally, IT operations management reviews audit reports and compliance documentation for third-party service providers on an annual basis to help ensure that relevant controls are in place and operating as intended to meet the organization's objectives and security, availability, and confidentiality commitments.

TRUST SERVICES CRITERIA AND RELATED CONTROL ACTIVITIES

Integration with Risk Assessment

Along with assessing risks, management has identified and put into effect actions needed to address those risks. In order to address risks, control activities have been placed into operation to help ensure that the actions are carried out properly and efficiently. Control activities serve as mechanisms for managing the achievement of the security, availability, processing integrity, and confidentiality categories.

Selection and Development of Control Activities

Selecting control activities includes consideration of the relevant business processes and identified risks that require control activities. Additionally, both automated and manual controls are considered during the selection of control activities. Management also considers how the environment, complexity, nature, and scope of its operations, as well as the specific characteristics of its organization, affect the selection and development of control activities. As part of this process, management also assigns risk owners to certain risks. The assigned risk owners select and develop control activities, including activities over technology, to mitigate the risks identified during the annual risk assessment process. The control activities are documented within the mitigation plans that are created by the risk owners for risks above the tolerable threshold.

Control activities are deployed through the use of policies to establish what is expected and procedures that put policies into action. Management has documented policies and procedures that guide personnel with regard to the design, development, implementation, operation, maintenance, and monitoring of in-scope systems. These policies and procedures are reviewed by management at least annually and communicated to internal personnel via the company intranet. Employees are held accountable for complying with these policies. An employee sanction procedure is in place that outlines the consequences for noncompliance.

The applicable trust services criteria and related control activities are included in Section 4 of this report to eliminate the redundancy that would result from listing the items in this section and repeating them in Section 4. Although the applicable trust services criteria and related control activities are included in Section 4, they are, nevertheless, an integral part of Stax's description of the system.

The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in Section 4, the Testing Matrices, adjacent to the service organization's description of controls. The description of the tests of operating effectiveness and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

Trust Services Criteria Not Applicable to the In-Scope System

All criteria within the security, availability, processing integrity, and confidentiality categories are applicable to the Stax, CardX and Stax Bill applications system.

INFORMATION AND COMMUNICATION SYSTEMS

Information and communication are integral components of Stax' internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, information technology. At Stax, information is identified, captured, processed, and reported by various information systems as well as through conversations with clients, vendors, regulators, and employees.

Internal Communications

Stax has implemented various methods of communication to help provide assurance that all employees understand their individual roles and responsibilities and that significant events are communicated. These methods include departmental and organizational meetings, documented policies and procedures, the employee handbook, job descriptions, and training made available to all employees. Employees must acknowledge that they have been given access to the employee handbook at the time of hire, and policies are published on the company intranet.

Technology all hands calls are held at least monthly to discuss changes to internal controls, metrics, and system updates. Architecture committee meetings are held on a weekly basis to discuss ongoing and upcoming projects for application and infrastructure changes. Additionally, a governance, risk and compliance steering committee is in place to monitor security, compliance, and internal policies and meet on a quarterly basis.

A security incident and event management (SIEM) system is in place to monitor and log security information and events related to the systems. Security assessments such as vulnerability assessments are also performed and results are reviewed to address identified vulnerabilities.

External Communications

Stax communicates the company's approach related to confidentiality through the company website via the privacy policy and terms of service. Stax provides customers with links containing updated information related to the usage and features of the products. Stax publishes information related to major releases to customers to educate them on changes and enhancements to the product. Company related announcements are communicated via the company website to enable communication of information to external parties. Knowledge articles are made

available to customers via the company website and include guides on how to use the system. A customer support service desk, e-mail and hotline are also made available to external users to report failures, incidents, and other complaints. Customer submitted requests are documented and tracked through resolution within an automated ticketing system.

MONITORING

Monitoring is a process that assesses the quality of internal control performance over time. It involves assessing the design and operation of controls and taking necessary corrective actions. This process is accomplished through ongoing activities, separate evaluation, or a combination of the two. Monitoring activities also include using information from communications from external parties such as user entity complaints and regulatory comments that may indicate problems or highlight areas in need of improvement. Stax has implemented a self-assessment and compliance program to help ensure the controls are consistently applied as designed.

Ongoing Monitoring and Separate Evaluation

Stax performs ongoing monitoring and separate evaluations to help ensure that business systems operate effectively on a continuous basis. Aspects of the ongoing monitoring procedures and separate evaluations include the following:

- Security reviews and vulnerability assessments are performed by third-party vendors including weekly vulnerability scans. Results are communicated to relevant parties and issues tracked and monitored through resolution.
- Management holds a quarterly business review meeting with executive management to discuss performance metrics and changes with regard to its business objectives and goals.
- The board of directors' meetings are held on a quarterly basis to review internal control performance, financials, regulatory, auditor report and communicate any issues identified.
- User access reviews, including licenses, software, and privileged users, are performed by management on a quarterly basis to help ensure that access to data is restricted and authorized. Accounts identified as inappropriate are investigated and resolved.
- Management assigns risk owners and selects and develops control activities to mitigate the risks identified during the annual risk assessment process. The control activities are documented within the mitigation plans that are created by the risk owners for risks above the tolerable threshold.
- IT operations management reviews audit reports and compliance documentation for third-party service providers on an annual basis to help ensure that relevant controls are in place and operating as intended to meet the organization's objectives and security, availability, and confidentiality commitments.

Subservice Organization Monitoring

On an annual basis, Stax receives and reviews the third-party attestation report provided by AWS and Rogers DC to help ensure it is in compliance with contractual obligations, and Stax' security requirements. Additionally, security and compliance personnel review security questionnaires completed by vendors and/or independent audit reports on an annual basis to evaluate the impact of any changes that could impact the organization's internal system of controls.

Evaluating and Communicating Deficiencies

Stax has developed incident handling procedures to report deficiencies and take corrective action. SIEM systems generate alerts for performance and availability and alerts are monitored in real time by information security personnel. The nature, timing, and extent of the internal and third-party reviews are documented and reviewed by the management on a quarterly basis. Deviations or deficiencies associated with controls with a level high risk assignment are immediately escalated to executive management for immediate correction action. Reported

incidents are reviewed in accordance with the documented incident procedures, and corrective action, if required, is assigned to an appropriate individual, and documented once those required actions are complete, as part of the incident management process. Management reviews the deviations and corrective actions during quarterly change management committee meetings.

COMPLEMENTARY CONTROL RESPONSIBILITIES AT USER ENTITIES

Stax's controls are designed to provide reasonable assurance that the principal service commitments and system requirements can be achieved without the implementation of complementary controls at user entities. As a result, complementary user entity controls are not required, or significant, to achieve the principal service commitments and system requirements based on the applicable trust services criteria.

However, in order for user entities to benefit from the Stax, Cardx and Stax Bill applications system and its controls, the following responsibilities should be considered by user entities:

#	Control Responsibilities to be Considered by User Entities	Related Applicable Trust Services Criteria
1.	User entities are responsible for ensuring that data input into the systems is complete and accurate.	PI1.2

SECTION 4

TESTING MATRICES

TESTS OF OPERATING EFFECTIVENESS AND RESULTS OF TESTS

Scope of Testing

This report on the controls relates to the Stax, CardX and Stax Bill application system provided by Stax. The scope of the testing was restricted to the Stax, CardX and Stax Bill application system and its boundaries as defined in Section 3. Schellman conducted the examination testing over the period September 1, 2022, through March 31, 2023.

Tests of Operating Effectiveness

The tests applied to test the operating effectiveness of controls are listed alongside each of the respective control activities within the Testing Matrices. Such tests were considered necessary to evaluate whether the controls were sufficient to provide reasonable, but not absolute, assurance that the applicable trust services criteria were achieved during the period. In selecting the tests of controls, Schellman considered various factors including, but not limited to, the following:

- The nature of the control and the frequency with which it operates;
- The control risk mitigated by the control;
- The effectiveness of entity-level controls, especially controls that monitor other controls;
- The degree to which the control relies on the effectiveness of other controls; and
- Whether the control is manually performed or automated.

The types of tests performed with respect to the operational effectiveness of the control activities detailed in this section are briefly described below:

Test Approach	Description
Inquiry	Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related control activity. This included in-person interviews, telephone calls, e-mails, web-based conferences, or a combination of the preceding.
Observation	Observed the relevant processes or procedures during fieldwork. This included, but was not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations relevant to the performance of control policies and procedures.
Inspection	Inspected the relevant audit records. This included, but was not limited to, documents, system configurations and settings, or the existence of sampling attributes, such as signatures, approvals, or logged events. In some cases, inspection testing involved tracing events forward to consequent system documentation or processes (e.g., resolution, detailed documentation, alarms, etc.) or vouching backwards for prerequisite events (e.g., approvals, authorizations, etc.).

Sampling

Consistent with American Institute of Certified Public Accountants (AICPA) authoritative literature, Schellman utilizes professional judgment to consider the tolerable deviation rate, the expected deviation rate, the audit risk, the characteristics of the population, and other factors, in order to determine the number of items to be selected in a sample for a particular test. Schellman, in accordance with AICPA authoritative literature, selected samples in such a way that the samples were expected to be representative of the population. This included judgmental selection methods, where applicable, to ensure representative samples were obtained.

System-generated population listings were obtained whenever possible to ensure completeness prior to selecting samples. In some instances, full populations were tested in cases including but not limited to, the uniqueness of the event or low overall population size.

Reliability of Information Provided by the Service Organization

Observation and inspection procedures were performed related to certain system-generated reports, listings, and queries to assess the accuracy and completeness (reliability) of the information used in the performance of our testing of the controls.

Test Results

The results of each test applied are listed alongside each respective test applied within the Testing Matrices. Test results not deemed as control deviations are noted by the phrase "No exceptions noted." in the test result column of the Testing Matrices. Any phrase other than the aforementioned, constitutes either a test result that is the result of non-occurrence, a change in the application of the control activity, or a deficiency in the operating effectiveness of the control activity. Testing deviations identified within the Testing Matrices are not necessarily weaknesses in the total system of controls, as this determination can only be made after consideration of controls in place at user entities and subservice organizations, if applicable, and other factors. Control considerations that should be implemented by subservice organizations, in order to complement the control activities and achieve the service commitments and system requirements are presented in the "Subservice Organizations" sections, respectively, within Section 3.

SECURITY CATEGORY

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Control Environment			
CC1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CC1.1.1	The employee handbook developed and communicated to the entire workforce contains the policies, procedures, and organizational approach for the organization, including mechanism used to hold individual contributors accountable for alignment with the company.	Inspected the employee handbook maintained on the company intranet site to determine that the employee handbook was developed and communicated to the entire workforce and contained the policies, procedures, and organizational approach for the organization, including mechanism used to hold individual contributors accountable for alignment with the company.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.1.2	Employees are required to acknowledge the employee handbook upon hire indicating they have been given access to the employee handbook and understand their responsibility for adhering to the associated policies and procedures.	Inspected the employee handbook acknowledgment for a sample of employees hired during the period to determine that each employee sampled acknowledged the employee handbook upon hire indicating they had been given access to the employee handbook and understood their responsibility for adhering to the associated policies and procedures.	No exceptions noted.
CC1.1.3	Background checks are performed on employees as a component of the hiring process to ensure candidates have sufficient qualifications and technical competency.	Inspected the background check for a sample of employees hired during the period to determine that background checks were performed for each employee sampled as a component of the hiring process to ensure candidates had sufficient qualifications and technical competency.	No exceptions noted.
CC1.2 COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
CC1.2.1	The board of directors responsibilities are formally documented in the board of directors charter.	Inspected the board of directors charter to determine that the board of directors responsibilities were formally documented in the board of directors charter.	No exceptions noted.
CC1.2.2	The board of directors' meetings are held on a quarterly basis to review internal control performance, financials, metrics, organization structure, auditor report and communicate any issues identified.	Inspected the board of directors' meeting invite and presentation for a sample of quarters during the period to determine that board of directors' meetings were held to review internal control performance, financials, metrics, organization structure, auditor report and communicate any issues identified for each quarter sampled.	No exceptions noted.
CC1.3 COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
CC1.3.1	The organizational structure, reporting lines, and authorities are defined in organizational charts, updated on an as-needed basis, and communicated to employees.	Inspected the organizational chart and location to determine that the organizational structure, reporting lines, and authorities were defined in organizational charts, updated during the period, and communicated to employees.	No exceptions noted.
CC1.3.2	Documented job descriptions are in place and include expectations and responsibility of employees for their organizational unit.	Inspected the job description for a sample of employees to determine that documented job descriptions were place and included expectations and responsibility of employees for their organizational unit for each employee sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.3.3	The board of directors' meetings are held on a quarterly basis to review internal control performance, financials, regulatory, auditor report and communicate any issues identified.	Inspected the board of directors' meeting invite and presentation for a sample of quarters during the period to determine that board of directors' meetings were held to review internal control performance, financials, metrics, organization structure, auditor report and communicate any issues identified for each quarter sampled.	No exceptions noted.
CC1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC1.4.1	HR documents the organizational approach within policies and procedures for performing workforce evaluations of employees.	Inspected the workforce evaluation policies and procedures to determine that HR documented the organizational approach within policies and procedures for performing workforce evaluations to employees.	No exceptions noted.
CC1.4.2	Organizational leaders perform performance evaluations annually to evaluate the employee against company values, role specific goals and other management defined goals.	Inspected the performance evaluation for a sample of employees to determine that organizational leaders performed performance evaluations during the period to evaluate the employee against company values, role specific goals and other management defined goals for each employee sampled.	No exceptions noted.
CC1.4.3	Background checks are performed on employees as a component of the hiring process to ensure candidates have sufficient qualifications and technical competency.	Inspected the background check for a sample of employees hired during the period to determine that background checks were performed for each employee sampled as a component of the hiring process to ensure candidates had sufficient qualifications and technical competency.	No exceptions noted.
CC1.4.4	Established talent management policies and procedure are in place which defines the requirements which need to be fulfilled, in order to be hired for a position within the company.	Inspected the recruiting policies and procedures to determine that established talent management policies and procedures were in place which defined requirements which needed to be fulfilled in order to be hired for a position within the company.	No exceptions noted.
CC1.4.5	Documented job descriptions are in place and include expectations and responsibility of employees for their organizational unit.	Inspected the job description for a sample of employees to determine that documented job descriptions were place and included expectations and responsibility of employees for their organizational unit for each employee sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.4.6	The entity maintains a centralized knowledge base with the information and training required by individual contributors to perform their work functions.	Inspected the centralized knowledge base to determine that the entity maintained a centralized knowledge base with the information required by individual contributors to perform their work functions.	No exceptions noted.
CC1.5 COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC1.5.1	The board of directors' meetings are held on a quarterly basis to review internal control performance, financials, regulatory, auditor report and communicate any issues identified.	Inspected the board of directors' meeting invite and presentation for a sample of quarters during the period to determine that board of directors' meetings were held to review internal control performance, financials, metrics, organization structure, auditor report and communicate any issues identified for each quarter sampled.	No exceptions noted.
CC1.5.2	Documented job descriptions are in place and include expectations and responsibility of employees for their organizational unit.	Inspected the job description for a sample of employees to determine that documented job descriptions were place and included expectations and responsibility of employees for their organizational unit for each employee sampled.	No exceptions noted.
CC1.5.3	Organizational leaders perform performance evaluations annually to evaluate the employee against company values, role specific goals and other management defined goals.	Inspected the performance evaluation for a sample of employees to determine that organizational leaders performed performance evaluations during the period to evaluate the employee against company values, role specific goals and other management defined goals for each employee sampled.	No exceptions noted.
CC1.5.4	The employee handbook developed and communicated to the entire workforce contains the policies, procedures, and organizational approach for the organization, including mechanism used to hold individual contributors accountable for alignment with the company.	Inspected the employee handbook maintained on the company intranet site to determine that the employee handbook was developed and communicated to the entire workforce and contained the policies, procedures, and organizational approach for the organization, including mechanism used to hold individual contributors accountable for alignment with the company.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.5.5	Employees are required to acknowledge the employee handbook upon hire indicating they have been given access to the employee handbook and understand their responsibility for adhering to the associated policies and procedures.	Inspected the employee handbook acknowledgment for a sample of employees hired during the period to determine that each employee sampled acknowledged the employee handbook upon hire indicating they had been given access to the employee handbook and understood their responsibility for adhering to the associated policies and procedures.	No exceptions noted.
Communication and Information			
CC2.1 COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
CC2.1.1	Documented information security policies and procedures are in place for information assets including hardware, data (at-rest, during processing, or in transmission), software, administrative authorities, mobile devices, and access provisioning.	Inspected the information security policies and procedures to determine that documented information security policies and procedures were in place for information assets including hardware, data (at-rest, during processing, or in transmission), software, administrative authorities, mobile devices, and access provisioning.	No exceptions noted.
CC2.1.2	The entity has developed knowledge base articles and other documentation to support multiple functions within the organization. The information is communicated to the relevant teams and is updated as needed.	Inquired of the VP of IT and security regarding knowledge base articles to determine that the entity developed knowledge base articles and other documentation to support multiple functions within the organization, and the information was communicated to the relevant teams and updated as needed.	No exceptions noted.
		Inspected the knowledge base articles and training material maintained on the company intranet to determine that the entity developed knowledge base articles and other documentation to support multiple functions within the organization and that the information was communicated and updated during the period.	No exceptions noted.
CC2.1.3	A SIEM application is utilized to monitor and log security events for the in-scope system and alert IT personnel when predefined conditions are met.	Inspected the SIEM configuration and an example alert issued during the period to determine that a SIEM application was utilized to monitor and log security events for the in-scope system and alert IT personnel when predefined conditions were met.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.1.4	Security reviews and vulnerability assessments are performed by third-party vendors including weekly vulnerability scans. Results are communicated to relevant parties and issues tracked and monitored through resolution.	Inspected the vulnerability scan results for a sample of weeks during the period and example vulnerability scan e-mails issued during the period to determine that vulnerability scans were performed on a weekly basis by a third-party vendor and that results were communicated to IT management and issues tracked and monitored through resolution for each week sampled.	No exceptions noted.
CC2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
CC2.2.1	The entity maintains a centralized knowledge base with the information and training required by individual contributors to perform their work functions.	Inspected the centralized knowledge base to determine that the entity maintained a centralized knowledge base with the information required by individual contributors to perform their work functions.	No exceptions noted.
CC2.2.2	Technology all hands calls are held at least monthly to discuss changes to internal controls, metrics, and system updates.	Inspected the recurring invite and the technology all hands slide deck for a sample of months during the period to determine that technology all hands calls were held to discuss changes to internal controls, metrics and system updates for each month sampled.	No exceptions noted.
CC2.2.3	Architecture committee meetings are held on a weekly basis to discuss ongoing and upcoming projects for application and infrastructure changes.	Inspected the architecture committee meeting invite and meeting discussion for a sample of weeks during the period to determine that an architecture committee meeting was held to discuss ongoing and upcoming projects for application and infrastructure changes for each week sampled.	No exceptions noted.
CC2.2.4	A governance, risk and compliance steering committee is in place to monitor security, compliance, and internal policies and meet on a quarterly basis.	Inspected the steering committee charter and meeting notes for a sample of quarters during the period to determine that a governance, risk, and compliance steering committee was in place to monitor security, compliance and internal policies and met for each quarter sampled.	No exceptions noted.
CC2.2.5	Documented job descriptions are in place and include expectations and responsibility of employees for their organizational unit.	Inspected the job description for a sample of employees to determine that documented job descriptions were place and included expectations and responsibility of employees for their organizational unit for each employee sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.2.6	A whistle-blower hotline is provided to enable anonymous or confidential communication when normal channels are inoperative or ineffective.	Inspected the employee handbook to determine that a whistle-blower hotline was provided to enable anonymous or confidential communication when normal channels were inoperative or ineffective.	No exceptions noted.
CC2.2.7	The board of directors' meetings are held on a quarterly basis to review internal control performance, financials, regulatory, auditor report and communicate any issues identified.	Inspected the board of directors' meeting invite and presentation for a sample of quarters during the period to determine that board of directors' meetings were held to review internal control performance, financials, metrics, organization structure, auditor report and communicate any issues identified for each quarter sampled.	No exceptions noted.
CC2.3 COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CC2.3.1	The entity's press releases, and website announcements are used to enable communication of relevant and timely information to external parties.	Inspected the company's website to determine that the entity's press releases, and website announcements were used to enable communication of relevant and timely information to external parties.	No exceptions noted.
CC2.3.2	The entity communicates the company approach related to confidentiality and changes to such approach through publicly facing privacy policy, and terms of service.	Inspected the company's website including the privacy policies and terms of service to determine that the entity communicated the company approach related to confidentiality and changes to such approach through publicly facing privacy policy, and terms of service.	No exceptions noted.
CC2.3.3	A system description including information regarding the design, operation and boundaries of the system is communicated to users upon request.	Inquired of the VP of IT and security regarding system descriptions to determine that a system description including information regarding the design, operation and boundaries of the system was communicated to users upon request.	No exception noted.
		Inspected the system description and an example e-mail request communication occurring during the review period to determine that a system description including information regarding the design, operation and boundaries of the system is communicated to users upon request.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.3.4	A customer support service desk is made available to external users to report systems failures, incidents, concerns, and other complaints. Customer requests are tracked, documented, and resolved within an automated ticketing system.	Inspected the customer support site, and example tickets issued during the period to determine that a customer service desk was made available to external users to report systems failures, incidents, concerns, and other complaints and customer requests were tracked, documented, and resolved within an automated ticketing system.	No exceptions noted.
CC2.3.5	The entity maintains a centralized knowledge base with the information and training required by individual contributors to perform their work functions.	Inspected the centralized knowledge base to determine that the entity maintained a centralized knowledge base with the information required by individual contributors to perform their work functions.	No exceptions noted.
Risk Assessment			
CC3.1 COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
CC3.1.1	Documented policies and procedures are in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.	Inspected the risk assessment policies and procedures to determine that documented policies and procedures were in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.	No exceptions noted.
CC3.1.2	A risk assessment is performed on an annual basis that considers the identification and assessment of risks relating to objectives. Risks that are identified are rated using a risk evaluation process and are documented, along with mitigation strategies for management review.	Inspected the most recent risk assessment to determine that a risk assessment was performed during the period that considered the identification and assessment of risks relating to the entity's objectives and that the risks identified were documented and rated using a risk evaluation process, along with mitigation strategies for management review.	No exceptions noted.
CC3.1.3	Management holds a quarterly business review meeting with executive management to discuss performance metrics and changes with regard to its business objectives and goals.	Inspected the quarterly business review meeting presentation for a sample of quarters during the period to determine that management held a business review meeting with executive management to discuss performance metrics and changes with regard to its business objectives and goals for each quarter sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.2 COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
CC3.2.1	Documented policies and procedures are in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.	Inspected the risk assessment policies and procedures to determine that documented policies and procedures were in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.	No exceptions noted.
CC3.2.2	Security reviews and vulnerability assessments are performed by third-party vendors including weekly vulnerability scans. Results are communicated to relevant parties and issues tracked and monitored through resolution.	Inspected the vulnerability scan results for a sample of weeks during the period and example vulnerability scan e-mails issued during the period to determine that vulnerability scans were performed on a weekly basis by a third-party vendor and that results were communicated to IT management and issues tracked and monitored through resolution for each week sampled.	No exceptions noted.
CC3.2.3	A risk assessment is performed on an annual basis that considers the identification and assessment of risks relating to objectives. Risks that are identified are rated using a risk evaluation process and are documented, along with mitigation strategies for management review.	Inspected the most recent risk assessment to determine that a risk assessment was performed during the period that considered the identification and assessment of risks relating to the entity's objectives and that the risks identified were documented and rated using a risk evaluation process, along with mitigation strategies for management review.	No exceptions noted.
CC3.3 COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
CC3.3.1	Documented policies and procedures are in place to guide personnel in identifying and assessing risks including the potential for fraud.	Inspected the risk assessment policies and procedures to determine that documented policies and procedures were in place to guide personnel in identifying and assessing risks including the potential for fraud.	No exceptions noted.
CC3.3.2	A risk assessment is performed on an annual basis that considers the potential for fraud. Risks that are identified are rated using a risk evaluation process and are formally documented for management review.	Inspected the most recent risk assessment to determine that a risk assessment was performed during the period that considered the potential for fraud and that risks identified were rated using a risk evaluation process and formally documented for management review.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.3.3	A fraud review meeting is held on a monthly basis to evaluate the potential fraud risk to the use of IT assets and access to information.	Inspected the fraud review meeting invites and agenda for a sample of months during the period to determine that a fraud review meeting was held to evaluate the potential fraud risk to the use of IT assets and access to information for each month sampled.	No exception noted.
CC3.4 COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC3.4.1	Documented policies and procedures are in place to guide personnel in the identification and assessment of relevant changes that could significantly impact the system of internal control.	Inspected the risk assessment policies and procedures to determine that documented policies and procedures were in place to guide personnel in the identification and assessment of relevant changes that could significantly impact the system of internal control.	No exceptions noted.
CC3.4.2	A risk assessment is performed on an annual basis that considers the impact of changes to the system. Risks that are identified are rated using a risk evaluation process and are formally documented for management review.	Inspected the most recent risk assessment to determine that a risk assessment was performed during the period that considered the impact of changes to the system and that risks identified were rated using a risk evaluation process and formally documented for management review.	No exceptions noted.
CC3.4.3	Management monitors the security risks of emerging technologies and the impact to the organization's services are considered by senior management.	Inquired of the VP of IT and security regarding the risk monitoring procedures to determine that management monitored the security risks of emerging technologies and the impact to the organization's services were considered by senior management.	No exceptions noted.
		Inspected example security bulletins and e-mail advisory notifications received during the period to determine that management personnel subscribed to security special interest groups and services to monitor the security risks and impacts of emerging technologies for consideration by senior management.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Monitoring Activities			
CC4.1 COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
CC4.1.1	Security reviews and vulnerability assessments are performed by third-party vendors including weekly vulnerability scans. Results are communicated to relevant parties and issues tracked and monitored through resolution.	Inspected the vulnerability scan results for a sample of weeks during the period and example vulnerability scan e-mails issued during the period to determine that vulnerability scans were performed on a weekly basis by a third-party vendor and that results were communicated to IT management and issues tracked and monitored through resolution for each week sampled.	No exceptions noted.
CC4.1.2	Management holds a quarterly business review meeting with executive management to discuss performance metrics and changes with regard to its business objectives and goals.	Inspected the quarterly business review meeting presentation for a sample of quarters during the period to determine that management held a business review meeting with executive management to discuss performance metrics and changes with regard to its business objectives and goals for each quarter sampled.	No exceptions noted.
CC4.1.3	The board of directors' meetings are held on a quarterly basis to review internal control performance, financials, regulatory, auditor report and communicate any issues identified.	Inspected the board of directors' meeting invite and presentation for a sample of quarters during the period to determine that board of directors' meetings were held to review internal control performance, financials, metrics, organization structure, auditor report and communicate any issues identified for each quarter sampled.	No exceptions noted.
CC4.1.4	User access reviews, including licenses, software, and privileged users, are performed by management on a quarterly basis to help ensure that access to data is restricted and authorized. Accounts identified as inappropriate are investigated and resolved.	Inquired of the VP of IT and security regarding user access reviews to determine that user access reviews were performed by management on a quarterly basis to help ensure that access to data is restricted and authorized, and that accounts identified as inappropriate were investigated and resolved.	No exceptions noted.
		Inspected the user access review documentation for a sample of quarters during the period to determine that user access reviews were performed by management to help ensure that access to data is restricted and authorized for each quarter sampled..	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.2 COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.			
CC4.2.1	Security reviews and vulnerability assessments are performed by third-party vendors including weekly vulnerability scans. Results are communicated to relevant parties and issues tracked and monitored through resolution.	Inspected the vulnerability scan results for a sampled of weeks during the period and example vulnerability scan e-mails issued during the period to determine that vulnerability scans were performed on a weekly basis by a third-party vendor and that results were communicated to IT management and issues tracked and monitored through resolution for each week sampled.	No exceptions noted.
CC4.2.2	The board of directors' meetings are held on a quarterly basis to review internal control performance, financials, regulatory, auditor report and communicate any issues identified.	Inspected the board of directors' meeting invite and presentation for a sample of quarters during the period to determine that board of directors' meetings were held to review internal control performance, financials, metrics, organization structure, auditor report and communicate any issues identified for each quarter sampled.	No exceptions noted.
CC4.2.3	Management assigns risk owners and selects and develops control activities over technology to mitigate the risks identified during the annual risk assessment process. The control activities are documented within the mitigation plans that are created by the risk owners for risks above the tolerable threshold.	Inspected the most recent risk assessment documentation to determine that management assigned risk owners, selected, and developed control activities over technology to mitigate the risks identified during the risk assessment process, and that control activities were documented within the mitigation plans that were created by the risk owners for risks above the tolerable threshold during the period.	No exceptions noted.
CC4.2.4	IT operations management reviews audit reports and compliance documentation for third-party service providers on an annual basis to help ensure that relevant controls are in place and operating as intended to meet the organization's objectives and security, availability, and confidentiality commitments.	Inquired of the VP of IT and security regarding the vendor management procedures to determine that IT operations management obtained and reviewed audit reports and compliance documentation for third-party service providers on an annual basis to help ensure the relevant controls were in place and operating as intended to meet the organization's objectives and security, availability, and confidentiality commitments.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the most recent third-party vendor compliance review documentation and the corresponding audit reports for a sample of vendors to determine that IT operations management obtained and reviewed audit reports and compliance documentation for each vendor sampled during the period.	No exceptions noted.
Control Activities			
CC5.1 COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
CC5.1.1	A risk assessment is performed on an annual basis that considers the identification and assessment of risks relating to objectives. Risks that are identified are rated using a risk evaluation process and are documented, along with mitigation strategies for management review.	Inspected the most recent risk assessment to determine that a risk assessment was performed during the period that considered the identification and assessment of risks relating to the entity's objectives and that the risks identified were documented and rated using a risk evaluation process, along with mitigation strategies for management review.	No exceptions noted.
CC5.1.2	Management assigns risk owners and selects and develops control activities to mitigate the risks identified during the annual risk assessment process. The control activities are documented within the mitigation plans that are created by the risk owners for risks above the tolerable threshold.	Inspected the most recent risk assessment documentation to determine that management assigned risk owners, selected, and developed control activities to mitigate the risks identified during the risk assessment process, and that control activities were documented within the mitigation plans that were created by the risk owners for risks above the tolerable threshold during the period.	No exceptions noted.
CC5.2 COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
CC5.2.1	Management assigns risk owners and selects and develops control activities over technology to mitigate the risks identified during the annual risk assessment process. The control activities are documented within the mitigation plans that are created by the risk owners for risks above the tolerable threshold.	Inspected the most recent risk assessment documentation to determine that management assigned risk owners, selected, and developed control activities over technology to mitigate the risks identified during the risk assessment process, and that control activities were documented within the mitigation plans that were created by the risk owners for risks above the tolerable threshold during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC5.3.1	Documented policies and procedures are in place to guide personnel with regard to the design, development, implementation, operation, maintenance, and monitoring of the in-scope systems. The policies and procedures are reviewed by management on an annual basis and communicated to internal personnel via the company intranet site.	Inspected the information security policies and procedures maintained on the company intranet site to determine that the documented policies and procedures were reviewed by management during the period and communicated internally via the company intranet site to guide personnel with regard to the design, development, implementation, operation, maintenance, and monitoring of the in-scope systems.	No exceptions noted.
CC5.3.2	Employee sanction policy statements are documented within the code of conduct and company policies to communicate consequences for policy and code violations, including disciplinary action, up to and including termination.	Inspected the code of conduct to determine that employee sanction policy statements were documented within the code of conduct and company policies to communicate consequences for policy and code violations, including disciplinary action, up to and including termination.	No exceptions noted.
CC5.3.3	Documented job descriptions are in place, communicated during the on-boarding process and include expectations and responsibilities of employees for their organizational unit.	Inspected the job description for a sample of employees to determine that documented job descriptions were in place and included expectations and responsibilities of employees for their organizational unit for each employee sampled.	No exceptions noted.
Logical and Physical Access Controls			
CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
CC6.1.1	Documented logical access policies and procedures are in place to guide personnel in information security practices to restrict access to information assets.	Inspected the access control policy to determine that documented logical access policies and procedures were in place to guide personnel in information security practices to restrict access to information assets.	No exceptions noted.
CC6.1.2	Configuration standards are in place for installation and maintenance of production servers including services, deployment, and hardening restrictions.	Inspected the configuration standards policy to determine that configuration standards were in place for installation and maintenance of production servers including services and application restrictions.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.1.3	The in-scope systems are configured to authenticate users with a unique user account and minimum password requirements or multi-factor authentication.	Inspected the user listing and password requirements for in-scope systems (AWS, servers, databases, applications) with the assistance of the VP of IT and security to determine that in-scope systems were configured to authenticate users with a unique user account and enforce predefined user account and minimum password requirements or multi-factor authentication.	No exceptions noted.
CC6.1.4	Predefined security groups are utilized to assign role-based access privileges and segregate access to in-scope systems.	Inspected the user access and group listing for in-scope systems (AWS, servers, databases, applications) with the assistance of the VP of IT and security to determine that predefined security groups are utilized to assign role-based access privileges and segregate access to data for the in-scope systems.	No exceptions noted.
CC6.1.6	The production network is segmented to help ensure that confidential data is isolated from other unrelated networks.	Inspected the network segmentation configuration to determine that the production network was segmented to help ensure that confidential data was isolated from other unrelated networks.	No exceptions noted.
	AWS is responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Stax application systems reside.		
CC6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
CC6.2.1	User access requests are documented in a ticketing system, and users are granted access based on the concept of least privilege using the access matrix.	Inquired of the vice president of IT and security regarding user access requests to determine that user access was granted based on the concept of least privilege based on their role.	No exceptions noted.
		Inspected the access ticket for a sample of employees hired during the period and the access matrix to determine that user access requests were documented in the ticketing system, and users were granted access based on the concept of least privilege using the access matrix for each employee sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.2.2	Termination requests are documented, and system access is revoked for employees as a component of the employee termination process.	Inspected the termination ticket for a sample of employees terminated during the period to determine that termination requests were documented, and system access was revoked as a component of the employee termination process for each employee sampled.	No exceptions noted.
		Inspected the user listings to in-scope systems (AWS, servers, databases, applications) with the assistance of the VP of IT and security for a sample of employees terminated during the period to determine that system access was revoked for the sampled employees as a component of the employee termination process.	No exceptions noted.
CC6.2.3	User access reviews, including licenses, software, and privileged users, are performed by management on a quarterly basis to help ensure that access to data is restricted and authorized. Accounts identified as inappropriate are investigated and resolved.	Inquired of the VP of IT and security regarding user access reviews to determine that user access reviews were performed by management on a quarterly basis to help ensure that access to data is restricted and authorized, and that accounts identified as inappropriate were investigated and resolved.	No exceptions noted.
		Inspected the user access review documentation for a sample of quarters during the period to determine that user access reviews were performed by management to help ensure that access to data is restricted and authorized for each quarter sampled.	No exceptions noted.
	AWS is responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Stax application systems reside.		
CC6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.			
CC6.3.1	User access requests are documented in a ticketing system, and users are granted access based on the concept of least privilege using the access matrix.	Inquired of the vice president of IT and security regarding user access requests to determine that user access was granted based on the concept of least privilege based on their role.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the access ticket for a sample of employees hired during the period and the access matrix to determine that user access requests were documented in the ticketing system, and users were granted access based on the concept of least privilege using the access matrix for each employee sampled.	No exceptions noted.
CC6.3.2	Termination requests are documented, and system access is revoked for employees as a component of the employee termination process.	Inspected the termination ticket for a sample of employees terminated during the period to determine that termination requests were documented, and system access was revoked as a component of the employee termination process for each employee sampled.	No exceptions noted.
		Inspected the user listings to in-scope systems (AWS, servers, databases, applications) with the assistance of the VP of IT and security for a sample of employees terminated during the period to determine that system access was revoked for the sampled employees as a component of the employee termination process.	No exceptions noted.
CC6.3.3	User access reviews, including licenses, software, and privileged users, are performed by management on a quarterly basis to help ensure that access to data is restricted and authorized. Accounts identified as inappropriate are investigated and resolved.	Inquired of the VP of IT and security regarding user access reviews to determine that user access reviews were performed by management on a quarterly basis to help ensure that access to data is restricted and authorized. Accounts identified as inappropriate were investigated and resolved.	No exceptions noted.
		Inspected the user access review documentation for a sample of quarters during the period to determine that user access reviews were performed by management for each quarter sampled.	No exceptions noted.
CC6.3.4	Administrative access privileges to the in-scope systems are restricted to user accounts accessible by authorized personnel.	Inquired of the vice president of IT and security regarding administrative access privileges to in-scope systems (AWS, servers, databases, applications) with the assistance of the VP of IT and security was restricted to authorized personnel.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the administrative access listings for a sample of in-scope systems (AWS, servers, databases, applications) with the assistance of the VP of IT and security to determine that administrative access privileges to the sampled in-scope systems were restricted to user accounts accessible by authorized personnel.	No exceptions noted.
	AWS is responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Stax application systems reside.		
CC6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.			
CC6.4.1	The physical security policy establishes the physical access requirements for office spaces, work area, and physical access removal.	Inspected the physical security policy to determine that a physical security policy established the physical access requirements for office spaces, work area and physical access removal.	No exceptions noted.
CC6.4.2	Physical access to the Stax Bill datacenter is granted only while required to perform a job function within the company.	Inspected the datacenter physical access user listing with the assistance of the VP of IT and Security to determine that physical access to the Stax Bill datacenter was granted only while required to perform a job function within the company.	No exceptions noted.
	AWS and Rogers are responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers.		
CC6.5 The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.			
CC6.5.1	Data and equipment disposal policies are in place to guide personnel in performing sanitization procedures on instances and physical assets where production data resides to ensure data and software is unrecoverable prior to retiring virtual and physical assets.	Inspected the data management policy to determine that data and equipment disposal policies were in place to guide personnel in performing sanitization procedures on instances and physical assets where production data resides to ensure data and software is unrecoverable prior to retiring virtual and physical assets.	No exceptions noted.
	AWS and Rogers are responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers.		

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC6.6.1	Firewall rules and security groups are in place to filter unauthorized inbound network traffic from the Internet and are configured to deny any type of network connection that is not explicitly authorized by a rule.	Inspected the firewall rules and security group configuration to determine that firewall rules and security groups were in place to filter unauthorized inbound network traffic from the internet and were configured to deny any type of network connection that is not explicitly authorized by a rule.	No exceptions noted.
CC6.6.2	A web application firewall is configured to monitor for potential intrusion attempts to the applications, log and alert security personnel when unusual activity is detected.	Inspected the web application firewall configuration to determine that a web application firewall was configured to monitor for potential intrusion attempts to the applications, log and alert security personnel when unusual activity was detected.	No exceptions noted.
CC6.6.3	An intrusion detection system is in place to monitor network traffic for potential intrusions and alert security personnel when unusual activity is detected.	Inspected the intrusion detection system configuration and an example alert received during the period to determine that an intrusion detection system was in place to monitor network traffic for potential intrusions and alert security personnel when unusual activity was detected.	No exceptions noted.
CC6.6.4	SFTP protocols are used for Stax to secure data transfers.	Inspected the SFTP configuration for Stax to determine that SFTP protocols were used for Stax to secure data transfers.	No exceptions noted.
CC6.6.5	An encrypted VPN is required for remote access to the production network to help ensure the security and integrity of the data passing over the public network.	Inspected the VPN configuration to determine that an encrypted VPN was required for remote access to the production network to help ensure the security and integrity of data passing over the public network.	No exceptions noted.
CC6.6.6	Web application traffic is encrypted using TLS encryption.	Inspected the encryption configuration to determine that web application traffic was encrypted using TLS encryption.	No exceptions noted.
	AWS is responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Stax application systems reside.		
CC6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.			
CC6.7.1	Firewall rules and security groups are in place to filter unauthorized inbound network traffic from the Internet and are configured to deny any type of network connection that is not explicitly authorized by a rule.	Inspected the firewall rules and security group configuration to determine that firewall rules and security groups were in place to filter unauthorized inbound network traffic from the internet and were configured to deny any type of network connection that is not explicitly authorized by a rule.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.7.2	A web application firewall is configured to monitor for potential intrusion attempts to the applications, log and alert security personnel when unusual activity is detected.	Inspected the web application firewall configuration to determine that a web application firewall was configured to monitor for potential intrusion attempts to the applications, log and alert security personnel when unusual activity was detected.	No exceptions noted.
CC6.7.3	SFTP protocols are used for Stax to secure data transfers.	Inspected the SFTP configuration for Stax to determine that SFTP protocols were used for Stax to secure data transfers.	No exceptions noted.
CC6.7.4	An encrypted VPN is required for remote access to the production network to help ensure the security and integrity of the data passing over the public network.	Inspected the VPN configuration to determine that an encrypted VPN was required for remote access to the production network to help ensure the security and integrity of data passing over the public network.	No exceptions noted.
CC6.7.5	Web application traffic is encrypted using TLS encryption.	Inspected the encryption configuration to determine that web application traffic was encrypted using TLS encryption.	No exceptions noted.
	AWS is responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices for its cloud hosting services where Stax systems reside.		
CC6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
CC6.8.1	A central endpoint detection and response solution is configured with antimalware software to detect, alert, and respond to cyber threats on production systems.	Inspected the endpoint detection and response (EDR) configuration, alert settings and enrolled devices to determine that a central endpoint detection and response solution was configured with antimalware software to detect, alert, and respond to cyber threats on production systems.	No exceptions noted.
CC6.8.2	A SIEM application is utilized to monitor and log security events for the in-scope system and alert IT personnel when predefined conditions are met.	Inspected the SIEM configuration and an example alert received during the period to determine that a SIEM application was utilized to monitor and log security events for the in-scope system and alert IT personnel when predefined conditions were met.	No exceptions noted.
CC6.8.3	Security reviews and vulnerability assessments are performed by third-party vendors including weekly vulnerability scans. Results are communicated to relevant parties and issues tracked and monitored through resolution.	Inspected the vulnerability scan results for a sample of weeks during the period and example vulnerability scan e-mails issued during the period to determine that vulnerability scans were performed on a weekly basis by a third-party vendor and that results were communicated to IT management and issues tracked and monitored through resolution for each week sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
System Operations			
CC7.1 To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.			
CC7.1.1	Configuration standards are in place for installation and maintenance of production servers including services, deployment, and hardening restrictions.	Inspected the configuration standards policy to determine that configuration standards were in place for installation and maintenance of production servers including services and application restrictions.	No exceptions noted.
CC7.1.2	Security reviews and vulnerability assessments are performed by third-party vendors including weekly vulnerability scans. Results are communicated to relevant parties and issues tracked and monitored through resolution.	Inspected the vulnerability scan results for a sample of weeks during the period and example vulnerability scan e-mails issued during the period to determine that vulnerability scans were performed on a weekly basis by a third-party vendor and that results were communicated to IT management and issues tracked and monitored through resolution for each week sampled.	No exceptions noted.
CC7.1.3	Firewall rules and security groups are in place to filter unauthorized inbound network traffic from the Internet and are configured to deny any type of network connection that is not explicitly authorized by a rule.	Inspected the firewall rules and security group configuration to determine that firewall rules and security groups were in place to filter unauthorized inbound network traffic from the internet and were configured to deny any type of network connection that is not explicitly authorized by a rule.	No exceptions noted.
CC7.1.4	A web application firewall is configured to monitor for potential intrusion attempts to the applications, log and alert security personnel when unusual activity is detected.	Inspected the web application firewall configuration to determine that a web application firewall was configured to monitor for potential intrusion attempts to the applications, log and alert security personnel when unusual activity was detected.	No exceptions noted.
CC7.1.5	A SIEM application is utilized to monitor and log security events for the in-scope system and alert IT personnel when predefined conditions are met.	Inspected the SIEM configuration and an example alert received during the period to determine that a SIEM application was utilized to monitor and log security events for the in-scope system and alert IT personnel when predefined conditions were met.	No exceptions noted.
	AWS is responsible for monitoring any changes to the logical access controls system for the underlying network, virtualization management, and storage devices where the Stax application systems reside.		

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
CC7.2.1	Enterprise monitoring applications are utilized to monitor the performance and availability of the production application and associated system resources. The monitoring applications are configured to send notifications to IT personnel when predefined thresholds are exceeded on monitored systems.	Inspected the system performance monitoring and alerting policy configurations for the enterprise monitoring applications and example alert notifications generated during the period to determine that enterprise monitoring applications were in place to monitor the performance and availability of the production application and associated system resources and were configured to send notifications to IT personnel when predefined thresholds were exceeded on monitored systems.	No exceptions noted.
CC7.2.2	Security reviews and vulnerability assessments are performed by third-party vendors including weekly vulnerability scans. Results are communicated to relevant parties and issues tracked and monitored through resolution.	Inspected the vulnerability scan results for a sample of weeks during the period and example vulnerability scan e-mails issued during the period to determine that vulnerability scans were performed on a weekly basis by a third-party vendor and that results were communicated to IT management and issues tracked and monitored through resolution for each week sampled.	No exceptions noted.
CC7.2.3	Firewall rules and security groups are in place to filter unauthorized inbound network traffic from the Internet and are configured to deny any type of network connection that is not explicitly authorized by a rule.	Inspected the firewall rules and security group configuration to determine that firewall rules and security groups were in place to filter unauthorized inbound network traffic from the internet and were configured to deny any type of network connection that is not explicitly authorized by a rule.	No exceptions noted.
CC7.2.4	A web application firewall is configured to monitor for potential intrusion attempts to the applications, log and alert security personnel when unusual activity is detected.	Inspected the web application firewall configuration to determine that a web application firewall was configured to monitor for potential intrusion attempts to the applications, log and alert security personnel when unusual activity was detected.	No exceptions noted.
	AWS is responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Stax application systems reside.		

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.			
CC7.3.1	An incident response policy is in place that provides guidance to personnel through incident reporting and procedures. The policy is made available to internal users via the intranet.	Inspected the incident response policy and intranet to determine that a formal incident response policy was in place that provided guidance to personnel through incident reporting and procedures and that the policy was readily available to internal users via the intranet.	No exceptions noted.
CC7.3.2	Reported or detected security incidents are tracked and reviewed by management and monitored through resolution.	Inspected the incident report for a sample of security incidents identified during the period to determine that each security incident sampled was tracked and reviewed by management and monitored through resolution.	No exceptions noted.
CC7.3.3	Corrective measures or changes that occur as a result of incidents and identified deficiencies follow the standard change control process.	Inquired of the VP of IT and security regarding corrective measures that occur as a result of incidents to determine that corrective measures or changes that occurred as a result of incidents and identified deficiencies followed the standard change control process.	No exceptions noted.
		Inspected the incident response plan and incident report for a sample of security incidents identified during the period to determine that corrective measures or changes that occurred as a result of incidents and identified deficiencies followed the standard change control process for each security incident sampled.	No exceptions noted.
CC7.3.4	Enterprise monitoring applications are utilized to monitor the performance and availability of the production application and associated system resources. The monitoring applications are configured to send notifications to IT personnel when predefined thresholds are exceeded on monitored systems.	Inspected the system performance monitoring and alerting policy configurations for the enterprise monitoring applications and example alert notifications generated during the period to determine that enterprise monitoring applications were in place to monitor the performance and availability of the production application and associated system resources and were configured to send notifications to IT personnel when predefined thresholds were exceeded on monitored systems.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.3.5	Events that resulted in unauthorized use or disclosure of confidential information or PII are communicated to the data subjects, legal and regulatory authorities, and others as required.	Inspected the notification procedures within the incident response plan to determine that events that resulted in unauthorized use or disclosure of confidential information or PII were communicated to the data subjects, legal and regulatory authorities, and others as required.	No exceptions noted.
CC7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
CC7.4.1	An incident response policy is in place that provides guidance to personnel through incident reporting and procedures. The policy is made available to internal users via the intranet.	Inspected the incident response policy and intranet to determine that a formal incident response policy was in place that provided guidance to personnel through incident reporting and procedures and that the policy was readily available to internal users via the intranet.	No exceptions noted.
CC7.4.2	Reported or detected security incidents are tracked and reviewed by management and monitored through resolution.	Inspected the incident report for a sample of security incidents identified during the period to determine that each security incident sampled was tracked and reviewed by management and monitored through resolution.	No exceptions noted.
CC7.4.3	Corrective measures or changes that occur as a result of incidents and identified deficiencies follow the standard change control process.	Inquired of the VP of IT and security regarding corrective measures that occur as a result of incidents to determine that corrective measures or changes that occurred as a result of incidents and identified deficiencies followed the standard change control process.	No exceptions noted.
		Inspected the incident response plan and incident report for a sample of security incidents identified during the period to determine that corrective measures or changes that occurred as a result of incidents and identified deficiencies followed the standard change control process for each security incident sampled.	No exceptions noted.
CC7.4.4	A root cause analysis is performed for incidents that includes an impact analysis, resolution, lessons learned, and action items, as needed.	Inspected the incident report for a sample of security incidents identified during the period to determine that a root cause analysis was performed for each security incident sampled and included an impact analysis, resolution, lessons learned, and action items as needed.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.4.5	Events that resulted in unauthorized use or disclosure of confidential information or PII are communicated to the data subjects, legal and regulatory authorities, and others as required.	Inspected the notification procedures within the incident response plan to determine that events that resulted in unauthorized use or disclosure of confidential information or PII were communicated to the data subjects, legal and regulatory authorities, and others as required.	No exceptions noted.
CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC7.5.1	Disaster recovery plan and tabletop testing activities are performed at least annually.	Inspected the most recent annual disaster recovery and tabletop testing plans and outputs to determine that disaster recovery plan and tabletop testing activities were performed during the period.	No exceptions noted.
CC7.5.2	Corrective measures or changes that occur as a result of incidents and identified deficiencies follow the standard change control process.	Inquired of the VP of IT and security regarding corrective measures that occur as a result of incidents to determine that corrective measures or changes that occurred as a result of incidents and identified deficiencies followed the standard change control process.	No exceptions noted.
		Inspected the incident response plan and incident report for a sample of security incidents identified during the period to determine that corrective measures or changes that occurred as a result of incidents and identified deficiencies followed the standard change control process for each security incident sampled.	No exceptions noted.
CC7.5.3	A root cause analysis is performed for incidents that includes an impact analysis, resolution, lessons learned, and action items, as needed.	Inspected the incident report for a sample of security incidents identified during the period to determine that a root cause analysis was performed for each security incident sampled and included an impact analysis, resolution, lessons learned, and action items as needed.	No exceptions noted.
CC7.5.4	Reported or detected security incidents are tracked and reviewed by management and monitored through resolution.	Inspected the incident report for a sample of security incidents identified during the period to determine that each security incident sampled was tracked and reviewed by management and monitored through resolution.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Change Management			
CC8.1 The entity authorizes, designs, develops, or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
CC8.1.1	The software development and change management policies and procedures are in place to document the formal approach used by the organization for managing system changes throughout the life cycle of the system.	Inspected the software development and change management policies and procedures to determine that software development and change management policies and procedures were in place to document the formal approach used by the organization for managing system changes throughout the life cycle of the system.	No exceptions noted.
CC8.1.2	Architecture committee meetings are held on a weekly basis to discuss ongoing and upcoming projects for application and infrastructure changes.	Inspected the architecture committee meeting invite and meeting discussion for a sample of weeks during the period to determine that an architecture committee meeting was held to discuss ongoing and upcoming projects for application and infrastructure changes for each week sampled.	No exceptions noted.
CC8.1.3	Application changes made to in-scope systems are authorized, tested, and approved by product management personnel prior to implementation within a ticketing system.	Inspected the change documentation for a sample of application changes completed during the period to determine that each change sampled was authorized, tested, and approved by product management personnel prior to implementation within a ticketing system.	No exceptions noted.
CC8.1.4	Infrastructure changes made to in-scope systems are documented within a ticketing system, approved and tested as needed.	Inspected the change documentation for a sample of infrastructure changes implemented during the period to determine that each infrastructure change sampled was documented within a ticketing system, approved and tested as needed.	The test of the control activity disclosed that two of 25 sampled infrastructure changes did not contain approval for system changes.
CC8.1.5	Version control software is utilized to restrict access to application source code and changes must be approved before being merge.	Inspected the version control user listing and configuration to determine that a version control software was utilized to restrict access to application source code and changes must be approved before being merged.	No exceptions noted.
CC8.1.6	Write access to the version control software is restricted to user accounts accessible by authorized personnel.	Inquired of the VP of IT and security regarding write access to the version control software to determine that write access to the version control software was restricted to user accounts by authorized personnel.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the users with write access to the version control software with the assistance of the VP of IT and security to determine that write access to the version control software was restricted to user accounts by authorized personnel.	No exceptions noted.
CC8.1.7	The production environments are logically segmented from the development and testing environments.	Inspected the segmentation configuration to determine that production environments were logically segmented from development and testing environments.	No exceptions noted.
CC8.1.8	The ability to approve and implement changes into the production environment is restricted to authorized personnel.	Inquired of the VP of IT and security regarding the ability to approve and implement changes to determine that the ability to approve and implement changes into the production environment was restricted to authorized personnel.	No exceptions noted.
		Inspected the listing of users with the ability to implement changes into the production environment with the assistance of the VP of IT and security to determine that the ability to approve and implement changes into the production environment was restricted to authorized personnel.	No exceptions noted.
CC8.1.9	Alerting tools are utilized to monitor for changes to the Stax, CardX, and Stax Bill production environments.	Inspected the alert configurations and example alerts generated during the period to determine that alerting tools were utilized to monitor for changes to the Stax, CardX, and Stax Bill production environments.	No exceptions noted.
CC8.1.10	Administrative access privileges within the alerting tools are segregated from those with development responsibility and restricted to user accounts accessible by authorized personnel.	Inspected the administrative access listing and privileges within the alerting tools with the assistance of the VP of IT and security to determine that administrative access privileges were segregated from those with development responsibility and restricted to user accounts accessible by authorized personnel.	The test of the control activity disclosed that administrative access privileges within the alerting tools were not segregated from those with development responsibility for three users within the Stax and CardX production environments. Additional testing of the control activity disclosed that the alert configurations were not modified during the period.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Risk Mitigation			
CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
CC9.1.1	Documented policies and procedures are in place to guide personnel in the identification, selection, and development of risk management activities for risks arising from potential business disruptions.	Inspected the risk assessment, business continuity and disaster recovery management policies and procedures to determine that documented policies and procedures were in place to guide personnel in the identification, selection, and development of risk management activities for risks arising from potential business disruptions.	No exceptions noted.
CC9.1.2	A risk assessment is performed on an annual basis that considers risks arising from potential business disruptions. Risks that are identified are rated using a risk evaluation process and are formally documented, along with mitigation strategies, for management review.	Inspected the most recent risk assessment to determine that a risk assessment was performed during the period that considered risks arising from potential business disruptions and that risks identified were rated using a risk evaluation process and formally documented, along with mitigation strategies, for management review.	No exceptions noted.
CC9.1.3	Disaster recovery plan and tabletop testing activities are performed at least annually.	Inspected the most recent annual disaster recovery and tabletop testing plans and outputs to determine that disaster recovery plan and tabletop testing activities were performed during the period.	No exceptions noted.
CC9.1.4	The organization considers the use of insurance to offset the financial impact of loss events that would otherwise impair the ability of the entity to meet its objectives.	Inspected the insurance policy documentation to determine that insurance was utilized to offset the financial impact of loss events that would otherwise impair the ability of the entity to meet its objectives.	No exceptions noted.
CC9.2 The entity assesses and manages risks associated with vendors and business partners.			
CC9.2.1	Vendor management policies are in place to guide personnel in the organization's data protection and handling requirements for third-party provider contracts and due diligence for the performance of periodic compliance monitoring activities.	Inspected the vendor management policies and procedures to determine that documented policies were in place to guide personnel in the organization's data protection and handling requirements for third-party provider contracts and due diligence activities for the performance of periodic compliance monitoring activities.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC9.2.2	A risk assessment is performed on an annual basis that considers risks associated with vendors and business partners. Risks that are identified are rated using a risk evaluation process and are formally documented, along with mitigation strategies, for management review.	Inspected the most recent risk assessment to determine that a risk assessment was performed during the period that considered risks associated with vendors and business partners and that risks identified were documented and rated using a risk evaluation process, along with mitigation strategies, for management review.	No exceptions noted.
CC9.2.3	IT operations management reviews audit reports and compliance documentation for third-party service providers on an annual basis to help ensure that relevant controls are in place and operating as intended to meet the organization's objectives and security, availability, and confidentiality commitments.	Inquired of the VP of IT and security regarding the vendor management procedures to determine that IT operations management obtained and reviewed audit reports and compliance documentation for third-party service providers on an annual basis to help ensure the relevant controls were in place and operating as intended to meet the organization's objectives and security, availability, and confidentiality commitments.	No exceptions noted.
		Inspected the most recent third-party vendor compliance review documentation and the corresponding audit reports for a sample of vendors to determine that IT operations management obtained and reviewed audit reports and compliance documentation for each vendor sampled during the period.	No exceptions noted.

ADDITIONAL CRITERIA FOR AVAILABILITY

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.1 The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.			
A1.1.1	Enterprise monitoring applications are utilized to monitor the performance and availability of the production application and associated system resources. The monitoring applications are configured to send notifications to IT personnel when predefined thresholds are exceeded on monitored systems.	Inspected the system performance monitoring and alerting policy configurations for the enterprise monitoring applications and example alert notifications generated during the period to determine that enterprise monitoring applications were in place to monitor the performance and availability of the production application and associated system resources and were configured to send notifications to IT personnel when predefined thresholds were exceeded on monitored systems.	No exceptions noted.
A1.1.2	A service status monitoring dashboard is made available via a public facing website to communicate current service availability, system uptime metrics, processing issues and outages is made available to end-users.	Inspected the status monitoring dashboard website, and the history logs for service interruptions and uptime availability metrics during the period to determine that a service status monitoring dashboard for the in-scope applications was in place that included communication of current service availability, system uptime metrics, processing issues and outages via a public facing website.	No exceptions noted.
A1.1.3	Architecture committee meetings are held on a weekly basis to discuss ongoing and upcoming projects for application and infrastructure changes.	Inspected the architecture committee meeting invite and meeting discussion for a sample of weeks during the period to determine that an architecture committee meeting was held to discuss ongoing and upcoming projects for application and infrastructure changes for each week sampled.	No exceptions noted.
A1.2 The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.			
A1.2.1	Documented policies and procedures are in place for responding to environmental threat events and for evaluating the effectiveness of those policies and procedures on an annual basis.	Inspected the incident response plan and risk assessment policy to determine that documented policies and procedures were in place to guide personnel in responding to environmental threat events and for evaluating the effectiveness of those policies and procedures on an annual basis.	No exception noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.2.2	An automated backup system is configured to perform daily backups of production data. The automated backup system is configured to log the backup job completion status for backups and send alert notifications to IT operations personnel regarding the failure of the backup jobs.	Inspected the automated backup system configurations and backup logs for a sample of databases to determine that an automated backup system was in place and configured to perform daily backups of production data, log the backup job completion statuses, and send alert notifications to IT personnel regarding the failure of the backup jobs for each database sampled.	No exception noted.
A1.2.3	Enterprise monitoring applications are utilized to monitor the performance and availability of the production application and associated system resources. The monitoring applications are configured to send notifications to IT personnel when predefined thresholds are exceeded on monitored systems.	Inspected the system performance monitoring and alerting policy configurations for the enterprise monitoring applications and example alert notifications generated during the period to determine that enterprise monitoring applications were in place to monitor the performance and availability of the production application and associated system resources and were configured to send notifications to IT personnel when predefined thresholds were exceeded on monitored systems.	No exceptions noted.
A1.2.4	Disaster recovery plan and tabletop testing activities are performed at least annually.	Inspected the most recent annual disaster recovery and tabletop testing plans and outputs to determine that disaster recovery plan and tabletop testing activities were performed during the period.	No exceptions noted.
A1.2.5	Production architecture is configured with redundancies to allow failover in the event of certain system failures or outages.	Inspected the network diagram and the high-availability configurations for a sample of production servers, databases, and network devices to determine that production architecture was configured with redundancies to allow failover in the event of certain system failures or outages.	No exceptions noted.
	AWS and Rogers are responsible for designing, developing, implementing, operating, maintaining, and monitoring the environmental control systems at the data center facility where the Stax application systems reside. AWS and Rogers are also responsible implementing recovery controls for failover to infrastructure located at an alternative facility in the event of a disaster or emergency event.		
A1.3 The entity tests recovery plan procedures supporting system recovery to meet its objectives.			
A1.3.1	Disaster recovery plan and tabletop testing activities are performed at least annually.	Inspected the most recent annual disaster recovery and tabletop testing plans and outputs to determine that disaster recovery plan and tabletop testing activities were performed during the period.	No exceptions noted.

ADDITIONAL CRITERIA FOR PROCESSING INTEGRITY

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
PI1.1 The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.			
PI1.1.1	The entity's security, availability, processing integrity, and confidentiality commitments and the associated system requirements are documented in customer contracts.	Inspected the customer contracts for a sample of customers to determine that the entity's security, availability, processing integrity, and confidentiality commitments and the associated system requirements were documented in customer contracts for each customer sampled.	No exceptions noted.
PI1.1.2	System processes and interfaces are documented to describe the design and operation of the system and its boundaries.	Inspected the system integration and technical process documentation for the in-scope applications to determine that system processes and interfaces were documented to describe the design and operation of the system and its boundaries.	No exceptions noted.
PI1.1.3	Transaction specifications and user guides, including required and recommended fields, are provided to customers to guide the users in the use of the services.	Inspected the guides and technical specifications documentation maintained on the in-scope application web portals to determine that transaction specifications and user guides, including required and recommended fields, were provided to customers to guide the users in the use of the services.	No exceptions noted.
PI1.1.4	The entity maintains a centralized knowledge base with the information and training required by individual contributors to perform their work functions.	Inspected the centralized knowledge base to determine that the entity maintained a centralized knowledge base with the information required by individual contributors to perform their work functions.	No exceptions noted.
PI1.1.5	Documented policies and procedures are in place to guide personnel in identifying and assessing risks related to transactional activity, including fraud.	Inspected the risk assessment policies and procedures to determine that documented policies and procedures were in place to guide personnel in identifying and assessing risks related to transactional activity, including fraud.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
PI1.2 The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives.			
PI1.2.1	Stax maintains a Data Management Policy which addresses the minimum system processing specifications necessary to meet its product or service objectives.	Inspected the data management policy documentation to determine that Stax maintained a Data Management Policy which addressed the minimum system processing specifications necessary to meet its product or service objectives.	No exceptions noted.
PI1.2.2	System processes and interfaces are documented to describe the design and operation of the system and its boundaries.	Inspected the system integration and technical process documentation for the in-scope applications to determine that system processes and interfaces were documented to describe the design and operation of the system and its boundaries.	No exceptions noted.
PI1.2.3	An implementation checklist is utilized to help ensure that consistent procedures are followed during the client implementation process for the in-scope applications.	Inspected the implementation checklist and onboarding documentation for a sample of clients onboarded during the period to determine that an implementation checklist was utilized to help ensure that consistent procedures are followed during the client implementation process for the in-scope applications for each client sampled.	No exceptions noted.
PI1.2.4	Enterprise monitoring and logging tools are configured to log user-related events to provide an audit trail of data input activities.	Inspected the enterprise monitoring and logging tool configurations and example logs generated by the system during the period to determine that the application was configured to log user-related events for data input activities and that an audit trail of the logged activities was in place.	No exceptions noted.
PI1.2.5	The enterprise monitoring and logging tools are configured to alert application support personnel regarding potential issues with system inputs (e.g., transactional activity).	Inspected the enterprise monitoring and logging tools automated alerting configurations and example system-generated alerts for system processing errors generated during the period to determine that the enterprise monitoring tools were configured to alert application support personnel regarding potential system errors during the processing of data.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
PI1.2.6	Data input and validation checks are in place to help ensure only valid data is entered into the application system.	Inspected the Stax, CardX and Stax Bill application configurations for example data input validation checks and the results of example transactions processed through the application user interface using valid and invalid data types to determine that data input and validation checks were in place for data entered into the application system.	No exceptions noted.
PI1.3 The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives.			
PI1.3.1	Data input and validation checks are in place to help ensure only valid data is entered into the application system.	Inspected the Stax, CardX and Stax Bill application configurations for example data input validation checks and the results of example transactions processed through the application user interface using valid and invalid data types to determine that data input and validation checks were in place for data entered into the application system.	No exceptions noted.
PI1.3.2	The enterprise monitoring and logging tools are configured to alert application support personnel regarding potential issues with transactional processing activities (e.g., unusual transactional volume, terminal security activity, unusual number of failed payments).	Inspected the enterprise monitoring and logging tools automated alerting configurations and example system-generated alerts for system processing errors generated during the period to determine that the enterprise monitoring tools were configured to alert application support personnel regarding potential issues with transactional processing activities (e.g., unusual transactional volume, terminal security activity, unusual number of failed payments).	No exceptions noted.
PI1.3.3	Enterprise monitoring applications are utilized to monitor the performance and availability of the production application and associated system resources. The monitoring applications are configured to send notifications to IT personnel when predefined thresholds are exceeded on monitored systems.	Inspected the system performance monitoring and alerting policy configurations for the enterprise monitoring applications and example alert notifications generated during the period to determine that enterprise monitoring applications were in place to monitor the performance and availability of the production application and associated system resources and were configured to send notifications to IT personnel when predefined thresholds were exceeded on monitored systems.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
PI1.3.4	A service status monitoring dashboard is made available via a public facing website to communicate current service availability, system uptime metrics, processing issues and outages is made available to end-users.	Inspected the status monitoring dashboard website, and the history logs for service interruptions and uptime availability metrics during the period to determine that a service status monitoring dashboard for the in-scope applications was in place that included communication of current service availability, system uptime metrics, processing issues and outages via a public facing website.	No exceptions noted.
PI1.4 The entity implements policies and procedures to make available or deliver output completely, accurately, and timely in accordance with specifications to meet the entity's objectives.			
PI1.4.1	Administrative access privileges to the in-scope systems are restricted to user accounts accessible by authorized personnel.	Inquired of the vice president of IT and security regarding administrative access privileges to in-scope systems (AWS, servers, databases, applications) with the assistance of the VP of IT and security was restricted to authorized personnel.	No exceptions noted.
		Inspected the administrative access listings for a sample of in-scope systems (AWS, servers, databases, applications) with the assistance of the VP of IT and security to determine that administrative access privileges to the sampled in-scope systems were restricted to user accounts accessible by authorized personnel.	No exceptions noted.
PI1.4.2	A service status monitoring dashboard is made available via a public facing website to communicate current service availability, system uptime metrics, processing issues and outages is made available to end-users.	Inspected the status monitoring dashboard website, and the history logs for service interruptions and uptime availability metrics during the period to determine that a service status monitoring dashboard for the in-scope applications was in place that included communication of current service availability, system uptime metrics, processing issues and outages via a public facing website.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
PI1.4.3	The enterprise monitoring and logging tools are configured to alert application support personnel regarding potential issues with transactional processing activities (e.g., unusual transactional volume, terminal security activity, unusual number of failed payments).	Inspected the enterprise monitoring and logging tools automated alerting configurations and example system-generated alerts for system processing errors generated during the period to determine that the enterprise monitoring tools were configured to alert application support personnel regarding potential issues with transactional processing activities (e.g., unusual transactional volume, terminal security activity, unusual number of failed payments).	No exceptions noted.
PI1.4.4	A fraud review meeting is held on a monthly basis to monitor sub-merchant customers for fraud or money laundering.	Inspected the fraud review meeting invites and agenda to determine that a fraud review meeting was held on a monthly basis to evaluate the potential fraud risk to the use of IT assets and access to information.	No exception noted.
PI1.5 The entity implements policies and procedures to store inputs, items in processing, and outputs completely, accurately, and timely in accordance with system specifications to meet the entity's objectives.			
PI1.5.1	Administrative access privileges to the in-scope systems are restricted to user accounts accessible by authorized personnel.	Inquired of the vice president of IT and security regarding administrative access privileges to in-scope systems (AWS, servers, databases, applications) with the assistance of the VP of IT and security was restricted to authorized personnel.	No exceptions noted.
		Inspected the administrative access listings for a sample of in-scope systems (AWS, servers, databases, applications) with the assistance of the VP of IT and security to determine that administrative access privileges to the sampled in-scope systems were restricted to user accounts accessible by authorized personnel.	No exceptions noted.
PI1.5.2	Production databases storing cardholder data are encrypted to help ensure confidential data is stored in an encrypted format.	Inspected the encryption configurations with the assistance of the VP of IT and security for a sample of production databases storing cardholder data to determine that production database servers storing cardholder data were configured to encrypt confidential data for each database server sampled.	No exception noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
PI1.5.3	A SIEM application is utilized to monitor and log security events for the in-scope system and alert IT personnel when predefined conditions are met.	Inspected the SIEM configuration and an example alert to determine that a SIEM application was utilized to monitor and log security events for the in-scope system and alert IT personnel when predefined conditions were met.	No exceptions noted.
PI1.5.4	User access reviews, including licenses, software, and privileged users, are performed by management on a quarterly basis to help ensure that access to data is restricted and authorized. Accounts identified as inappropriate are investigated and resolved.	Inquired of the VP of IT and security regarding user access reviews to determine that user access reviews were performed by management on a quarterly basis to help ensure that access to data is restricted and authorized. Accounts identified as inappropriate were investigated and resolved.	No exceptions noted.
		Inspected the user access review documentation for a sample of quarters during the period to determine that user access reviews were performed by management for each quarter sampled.	No exceptions noted.
PI1.5.5	An automated backup system is configured to perform daily backups of production data. The automated backup system is configured to log the backup job completion status for backups and send alert notifications to IT operations personnel regarding the failure of the backup jobs.	Inspected the automated backup system configurations and backup logs for a sample of databases to determine that an automated backup system was in place and configured to perform daily backups of production data, log the backup job completion statuses, and send alert notifications to IT personnel regarding the failure of the backup jobs for each database sampled.	No exception noted.
PI1.5.6	Production architecture is configured with redundancies to allow failover in the event of certain system failures or outages.	Inspected the network diagram and the high-availability configurations for a sample of production servers, databases, and network devices to determine that production architecture was configured with redundancies to allow failover in the event of certain system failures or outages.	No exceptions noted.

ADDITIONAL CRITERIA FOR CONFIDENTIALITY

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
C1.1 The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.			
C1.1.1	Documented data retention and disposal policies are in place to guide personnel on the procedures for retention and disposal of data and are updated annually.	Inspected the data retention and disposal policies to determine that documented data retention and disposal policies were in place to guide personnel on the procedures for retention and disposal of data and were updated during the period.	No exception noted.
C1.1.2	Production databases storing cardholder data are encrypted to help ensure confidential data is stored in an encrypted format.	Inspected the encryption configurations with the assistance of the VP of IT and security for a sample of production databases storing cardholder data to determine that production database servers storing cardholder data were configured to encrypt confidential data for each database server sampled.	No exception noted.
C1.1.3	Confidentiality agreements are required to be in place with third-party providers that may have access to personal information.	Inspected the confidentiality agreements for a sample of third-party providers with access to confidential information to determine that confidentiality agreements were in place for each third-party provider sampled.	No exception noted.
C1.1.4	IT operations management reviews audit reports and compliance documentation for third-party service providers on an annual basis to help ensure that relevant controls are in place and operating as intended to meet the organization's objectives and security, availability, and confidentiality commitments.	Inquired of the VP of IT and security regarding the vendor management procedures to determine that IT operations management obtained and reviewed audit reports and compliance documentation for third-party service providers on an annual basis to help ensure the relevant controls were in place and operating as intended to meet the organization's objectives and security, availability, and confidentiality commitments.	No exception noted.
		Inspected the most recent third-party vendor compliance review documentation and the corresponding audit reports for a sample of vendors to determine that IT operations management obtained and reviewed audit reports and compliance documentation for each vendor sampled during the period.	No exception noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
C1.2 The entity disposes of confidential information to meet the entity's objectives related to confidentiality.			
C1.2.1	Documented data retention and disposal policies are in place to guide personnel on the procedures for retention and disposal of data and are updated annually.	Inspected the data retention and disposal policies to determine that documented data retention and disposal policies were in place to guide personnel on the procedures for retention and disposal of data and were updated during the period.	No exceptions noted.
C1.2.2	Client data is disposed of upon request or termination of contract.	Inquired of the VP of IT and security regarding data disposal to determine that client data was disposed of upon customer request or upon termination of contract.	No exceptions noted.
		Inspected the deletion tickets for a sample of customer data deletion requests completed during the period to determine that client data was disposed of upon request or upon termination of contract for each data deletion request sampled.	No exceptions noted.

SECTION 5

OTHER INFORMATION PROVIDED BY STAX

MANAGEMENT'S RESPONSE TO TESTING EXCEPTIONS

Security Category

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC8.1.4	Infrastructure changes made to in-scope systems are documented within a ticketing system, approved and tested as needed.	Inspected the change documentation for a sample of infrastructure changes implemented during the period to determine that infrastructure changes made to in-scope systems were documents within a ticketing system, approved and tested as needed.	The test of the control activity disclosed that two of 25 sampled infrastructure changes did not contain approval for system changes.
Management's Response:	Functional teams were restructured during the period resulting in adjustments in responsibilities responsible for the gap in process. The process has been remediated, automated and manual steps have been implemented and documented to prevent reoccurrence.		

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC8.1.10	Administrative access privileges within the alerting tools are segregated from those with development responsibility and restricted to user accounts accessible by authorized personnel.	Inspected the administrative access listing and privileges within the alerting tools with the assistance of the VP of IT and security to determine that administrative access privileges were segregated from those with development responsibility and restricted to user accounts accessible by authorized personnel.	The test of the control activity disclosed that administrative access privileges within the alerting tools were not segregated from those with development responsibility for three users within the Stax and CardX production environments. Additional testing of the control activity disclosed that the alert configurations were not modified during the period.
Management's Response:	The three individuals listed are executive department leaders which were the system owners of the systems identified during the audit. The access has been segmented as a result of the finding to provide improved separation of duties.		